 https://doi.org/10.34836/pk.2021.314.2

Krajowa koncepcja rozwiązań systemowych w obszarze zwalczania wykorzystywania seksualnego dzieci

podinsp. w st. spocz. mgr Katarzyna Staciwa[1]

[1] NASK – Państwowy Instytut Badawczy, Dział Reagowania na Nielegalne Treści w Internecie Dyżurnet.pl, katarzyna.staciwa@nask.pl, ORCID: 0000-0003-0633-4696

Streszczenie

Wykorzystywanie seksualne dzieci w cyberprzestrzeni, w tym obecność treści będących wizualnym zapisem czynów zabronionych popełnionych na ich szkodę, to problem globalny. Walka z tym problemem jest skuteczna wtedy, gdy zaangażowane w nią podmioty korzystają w sposób systemowy z dostępnych rozwiązań technologicznych. Dotyczy to przede wszystkim tych rozwiązań, dzięki którym możliwa jest szybka weryfikacja, czy potencjalnie nielegalne treści zostały wcześniej sklasyfikowane jako przedstawiające wykorzystywanie seksualne dzieci (ang. *Child Sexual Abuse Material*, dalej: CSAM), jak również komunikacja pomiędzy podmiotami mającymi dostęp do takich treści w ramach wykonywanych obowiązków.
Niniejsze opracowanie ma na celu przybliżenie rozwiązań i narzędzi stosowanych w tym obszarze, zarówno na poziomie międzynarodowym, jak i krajowym, oraz przedstawienie propozycji podejścia systemowego, które przyczyni się do zwiększenia efektywności aktualnych rozwiązań w powyższym zakresie, na poziomie krajowym.

Słowa kluczowe: wykorzystywanie seksualne dzieci, cyberprzestrzeń, *Child Sexual Abuse Material, CSAM,* wartości *hash*

Wstęp

Ekspansja sieci komputerowej Internet w ostatnich latach, jak również rosnąca liczba komunikujących się z nią mobilnych urządzeń miały niewątpliwie wpływ na wiele obszarów funkcjonowania dzisiejszego społeczeństwa, nie bez powodu określanego jako globalna wioska. Postęp technologiczny, będący obecnie nieodłączną częścią naszego życia, spowodował, że wiele zjawisk występujących w realnym świecie przeniosło się do cyberprzestrzeni. Jak trafnie zauważa J. Wasilewski, istotę tej ostatniej „tworzy koncepcja powołania do życia swojego rodzaju równoległego środowiska, które jest nowym wymiarem dla ludzkich działań" (2013). Wskazany tutaj trend dotyczy również zjawiska wykorzystywania seksualnego dzieci, w przypadku którego rzeczywiste zachowania są utrwalane na zdjęciach i filmach wideo, dystrybuowanych następnie drogą cyfrową pomiędzy odbiorcami zaliczającymi się do szczególnej kategorii użytkowników cyberprzestrzeni.

Wymiary offline i online zostały tu ze sobą połączone w szczególny sposób. Związek ten opisali w swoich badaniach np. Seto, Hanson i Babchishin (2010), wskazując na to, że ok 55% sprawców działających w świecie wirtualnym przyznało się do wykorzystywania seksualnego dzieci w rzeczywistości a 12% takich sprawców miało wcześniejsze notowania kryminalne w związku z tzw. przestępstwami kontaktowymi. Z kolei amerykańska organizacja non-profit, Child Rescue Coalition (dalej: CRC), znana z dostarczania rozwiązań technologicznych wspierających organy ścigania, wskazuje na odsetek tzw. sprawców kontaktowych w grupie sprawców działających w świecie wirtualnym na poziomie 85% (2021).

Dla zobrazowania skali tego zjawiska warto w tym miejscu przywołać fakty dotyczące platform darknetowych, zlikwidowanych w wyniku międzynarodowych operacji organów ścigania w 2017 r.[1] Platformy te skupiały osoby zainteresowane seksualnie dziećmi, umożliwiając im bezpośrednią komunikację, w tym dystrybucję CSAM i transmisję wykorzystywania seksualnego dzieci w czasie rzeczywistym, nacechowane wysokim stopniem anonimowości. Zgodnie z informacjami przekazanymi przez działające w strukturach Agencji Unii Europejskiej ds. Współpracy Organów Ścigania z siedzibą w Hadze (dalej: Europol) Europejskie Centrum ds. Zwalczania Cyberprzestępczości (dalej: EC3), platformy te liczyły od kilkudziesięciu tysięcy użytkowników (platforma Elysium, ponad 87 000

[1] Dark web – to w dużym uproszczeniu ukryta część zasobów Internetu, którą można przeglądać za pomocą specjalnego oprogramowania. Natomiast Darknet to sieci o ograniczonym dostępie, składające się z wielu rozproszonych, anonimowych węzłów (takich jak Tor, I2P czy Freenet) umożliwiających wejście do Dark web.

użytkowników) do nawet kilkuset tysięcy (platforma Playpen, ponad 150 000), (2017).

Informacje o aktualnych trendach dotyczących zjawiska wykorzystywania seksualnego dzieci w cyberprzestrzeni można zaczerpnąć z raportów publikowanych przez wyspecjalizowane w tej dziedzinie agencje i organizacje, takie jak Europol, (2020 i 2021) czy Rada Europy (2021). W raportach tych, można zaobserwować podział trendów na:

- trendy dotyczące treści z kategorii CSAM oraz
- trendy dotyczące zachowań w cyberprzestrzeni (np. uwodzenie, nagabywanie, czy szantaż na tle seksualnym).

Wyniki analizy tych trendów dają podstawy do sformułowania wniosku, iż zjawisko wykorzystywania seksualnego dzieci nigdy nie zostanie całkowicie wyeliminowane z cyberprzestrzeni, natomiast można i należy dążyć do ograniczenia jego zasięgu i skali, choć i to zadanie jest już niewątpliwie ogromnym wyzwaniem. Dążenia te realizowane są w przeważającej mierze dzięki stosowaniu rozwiązań umożliwiających szybką weryfikację, czy potencjalnie nielegalne treści zostały już wcześniej sklasyfikowane jako CSAM, jak również komunikację pomiędzy podmiotami mającymi dostęp do takich treści w ramach wykonywanych obowiązków. Należy także odnotować, iż podejmowane są próby wdrażania rozwiązań wykorzystujących sztuczną inteligencję, mających na celu identyfikację niebezpiecznych dla dzieci zachowań online, takich jak uwodzenie (ang. *grooming*), (Microsoft, 2020). W tym opracowaniu przybliżono – w oparciu o metodę analizy i krytyki piśmiennictwa – funkcjonowanie rozwiązań nawiązujących do pierwszego z wymienionych powyżej trendów, jak również zaproponowano systemowe podejście, mogące poprawić efektywność aktualnych rozwiązań w tym obszarze w Polsce.

CSAM jako aktualne wyzwanie

Rozważania na temat pierwszego z wymienionych wcześniej trendów należy zacząć od sformułowania tezy, iż zapotrzebowanie na dostępność treści przedstawiających wykorzystywanie seksualnie dzieci w cyberprzestrzeni istnieje np. wtedy, kiedy użytkownikami tego wymiaru są osoby seksualnie nimi zainteresowane, a zwłaszcza mające warunki do tego, aby popełniać czyny zabronione o podłożu seksualnym i utrwalać je na materiałach audiowizualnych. Choć przedstawienie pełnej charakterystyki takich osób wykracza poza ramy tego opracowania, warto w tym miejscu zaznaczyć, iż posiadanie przez nie nowego, niepublikowanego wcześniej nigdzie indziej zdjęcia lub filmu z kategorii CSAM jest dla nich swego rodzaju trofeum oraz walutą (Europol, 2015). Posługiwanie się tą ostatnią może np. umożliwić „awans" w hierarchii działających w ukrytej części Internetu forów lub uzyskanie dostępu do grup zamkniętych, w ramach których rozpowszechniane są, włączając w to transmisje na żywo, ściśle określone treści, często przedstawiające najbardziej brutalne i sadystyczne traktowanie wykorzystywanego seksualnie dziecka.

Nie sposób oszacować, jaka ilość CSAM jest obecnie dostępna w cyberprzestrzeni. W swoich ostatnich publikacjach Europol po raz kolejny wskazuje na utrzymujący się z roku na rok wzrost ilości treści z kategorii CSAM ujawnionych w cyberprzestrzeni, co naturalnie przekłada się na ich ciągłą dystrybucję i redystrybucję (Europol, 2020). Jak szacują inni eksperci w tej dziedzinie, jedno zdjęcie lub film przedstawiający seksualne wykorzystywanie dziecka może być oglądane lub udostępniane w Internecie nawet do 70 000 razy (Web-IQ, 2020). Kolejnego punktu odniesienia w dążeniach do określenia skali problemu może dostarczyć liczba przekraczająca 2,5 miliona – dotyczy ona adresów IP, które zostały powiązane z jednym z najczęściej udostępnianych w cyberprzestrzeni plików z kategorii CSAM (CRC, 2021).

Organizacją o szczególnym mandacie w zakresie zapobiegania i zwalczania wykorzystywania seksualnego dzieci jest National Center for Missing & Exploited Children w Stanach Zjednoczonych (dalej: NCMEC). Posiada ona w swoich zasobach CyberTipline, tj. infolinię zrzeszoną – podobnie jak pozostałe 50 infolinii działających w różnych częściach świata – w stowarzyszeniu INHOPE (INHOPE, 2021). Zgodnie z amerykańskim prawem federalnym, lokalne podmioty sektora prywatnego mają obowiązek raportowania do CyberTipline przypadków ujawnienia w ich zasobach treści, mogących przedstawiać wykorzystywanie seksualnie dzieci. Jest to wyjątkowa regulacja, niemająca do tej pory swojego odpowiednika nigdzie indziej na świecie. Liczby publikowane przez tę organizację są alarmujące: w 2020 r. CyberTipline otrzymała ponad 21,7 milionów takich raportów, co stanowi 28% przyrost w porównaniu do roku 2019 (2020). W roku 2021 nastąpił kolejny wzrost liczby raportów – do 29,3 milionów (o 35% w stosunku do roku 2020), (NCMEC, 2022).

Charakterystykę wyzwania, jakim jest obecność CSAM w cyberprzestrzeni, należy zakończyć przywołaniem perspektywy osób pokrzywdzonych w wyniku przestępstwa z tej kategorii. Przeprowadzone badania z udziałem tych osób niejednokrotnie wykazywały, że dystrybucja CSAM drogą cyfrową pogłębia ich wiktymizację i ma na nie długotrwały, szkodliwy wpływ nawet wtedy, gdy osiągną już dorosłość (np. Canadian Centre for Child Protection, 2017). Zgodnie z wynikami ankiety przeprowadzonej przez to centrum, 70 % takiej populacji niezmiennie obawia się bycia rozpoznanym w życiu codziennym. Obowiązkiem społeczeństwa, w którym dorastają dzieci, jest więc nie tylko ich ochrona przed wykorzystywaniem seksualnym w rzeczywistym świecie, ale również przed doświadczaniem przez nie wtórnej wiktymizacji, spowodowanej dostępnością w świecie wirtualnym dowodów popełnienia wobec nich czynu zabronionego.

Technologia na służbie

Weryfikacja potencjalnie nielegalnych treści za pomocą porównywania nadanych im wartości *hash*, nie należy do nowych rozwiązań. Zastosowanie tej metody w zapobieganiu i zwalczaniu wykorzystywania seksualnego dzieci było już przedmiotem licznych publikacji naukowych (np. Quayle, 2020; Lee, Ermakova, Ververis, Fabian, 2020; Elshenraki, 2021), jak również eksperckich (np. Komisja Europejska, 2020; Rada Europy, 2021). Niniejsze opracowanie wykorzystuje treści pochodzące z takich publikacji, koncentrując się na praktycznej stronie stosowania tej metody jako kluczowego elementu w systemowym podejściu, które mogłoby zostać wdrożone na poziomie krajowym w Polsce.

Dogłębna analiza procesów związanych z nadawaniem wartości *hash* nie jest celem tego opracowania. W tym miejscu przydatne będzie jednak wyjaśnienie, że taka wartość to nic innego jak ciąg cyfr i znaków obliczanych za pomocą różnych algorytmów (np. MD5, SHA-1, PhotoDNA, pHash, TMK PDQF, SIFT), (np. Staciwa, 2021; Rada Europy, 2021), dlatego bardziej precyzyjnymi określeniami będą: wartość jednokierunkowej funkcji szyfrującej lub wartość kryptograficznej funkcji skrótu. Z racji tego, że wartość *hash* jest unikalna dla każdego pliku, jest ona równie często określana jako „cyfrowy odcisk palca".

Posługiwanie się opisywaną tutaj metodą jest niezwykle cenne dla wszystkich podmiotów zaangażowanych w identyfikację dzieci będących ofiarami wykorzystywania seksualnego oraz zwalczanie dostępności CSAM w cyberprzestrzeni. To dzięki niej możliwe jest szybkie ustalenie, czy w dużym zbiorze materiałów cyfrowych znajdują się treści z kategorii CSAM. Weryfikacja odbywająca się tą metodą jest podstawą funkcjonowania specjalnej bazy danych znajdującej się w zasobach Międzynarodowej Organizacji Policji INTERPOL z siedzibą Sekretariatu Generalnego w Lyonie (ang. *International Child Sexual Exploitation Database*, dalej: ICSE DB). ICSE DB to przede wszystkim platforma pozwalająca śledczym z ponad 68 krajów świata wymieniać się informacjami wywiadu kryminalnego o prowadzonych przez nich sprawach. Transfer treści do ICSE DB umożliwia sprawdzenie, czy takie treści zostały już zidentyfikowane w innym kraju, jak również czy noszą cechy podobieństwa do innych treści znajdujących się już w bazie danych, liczącej na dzień dzisiejszy ponad 4,3 milionów zdjęć i filmów wideo (INTERPOL, 2022). Opisywana tu weryfikacja jest dla śledczych bezcenna, oznacza bowiem możliwość ustalenia, czy materiały, którymi się zajmują, są nowe, co uzasadnia podejrzenie wykorzystywania seksualnego dziecka w czasie rzeczywistym i wiąże się z nadaniem takiemu przypadkowi odpowiedniego priorytetu. Częścią ICSE DB jest oprogramowanie, które porównuje zdjęcia i wideo, przez co śledczy mogą na bieżąco ustalać powiązania pomiędzy ofiarami, sprawcami i miejscami zdarzeń. Argumentem przemawiającym za słusznością stosowania omawianych tu rozwiązań powinien być fakt, iż współpraca międzynarodowej społeczności śledczych od początku istnienia ICSE DB doprowadziła do identyfikacji 32 700 dzieci na całym świecie (INTERPOL, 2023).

Dodatkowa korzyść wynikająca z opisywanej tu klasyfikacji jest taka, że osoba zajmująca się potencjalnie nielegalnymi treściami nie będzie musiała oglądać po raz kolejny treści, które zostały już wcześniej sklasyfikowane, co w praktyce sprowadza się nie tylko do uniknięcia powielania pracy osób obcujących z takimi treściami, ale również ograniczenia czasu, w jakim mają one z nimi kontakt. Obcowanie z tak szczególnymi treściami należy do wysoce obciążających, dlatego też mając na uwadze troskę o stan psychiczny i fizyczny takich osób, kontakt z nimi powinien być ograniczony do niezbędnego minimum.

Tworzenie wiarygodnych list wartości *hash* przypisanych treściom z kategorii CSAM oraz wymiana informacji o tych wartościach są nieocenionym wkładem w starania międzynarodowej społeczności zaangażowanej w przeciwdziałanie dostępności CSAM w cyberprzestrzeni. Wiedza i doświadczenie osób obcujących z tego rodzaju treściami w ramach wykonywanych obowiązków służbowych, nabywane m.in. na szkoleniach organizowanych przez INTERPOL, jak również możliwość współpracy z innymi podmiotami na poziomie globalnym, to elementy zwiększające skuteczność tych starań.

Warto w tym miejscu dodać, że rozwiązania oparte na opisywanej tutaj technologii są już od dawna stosowane przez niektóre organy ścigania, zwłaszcza te, które posiadają w swoich zasobach krajowe bazy CSAM, np. szwedzkie czy brytyjskie, jak również te, które na co dzień współpracują w ramach ICSE DB. Listę podmiotów wykorzystujących wartości *hash* w codziennej pracy uzupełniają ponadto niektóre z infolinii, zaangażowanych w usuwanie nielegalnych treści z cyberprzestrzeni: CyberTipline – Stany Zjednoczone, Cybertip!ca – Kanada, Internet Watch Foundation (dalej: IWF) – Wielka Brytania oraz, od niedawna, także Meldpunt Kinderporno – Holandia. Właśnie te podmioty podejmują ponadto działania mające na celu maksymalne wykorzystanie potencjału, jakim jest wiedza o sklasyfikowanych wcześniej treściach z kategorii CSAM. W przypadku IWF należy wymienić projekty IntelliGrade oraz IWF Crawler (IWF, 2022), natomiast odnośnie jej kanadyjskiej odpowiedniczki Cybertip!ca będzie to projekt Arachnid (Cybertip!ca, 2022). Wymienione tu przedsięwzięcia łączy ponadto dążenie do sklasyfikowania jak największej ilości treści, aby bazy referencyjne wartości *hash* były możliwie kompletne.

Posługiwanie się wartościami *hash* to rozwiązanie przynoszące wiele korzyści, jednak obszar ten wymaga również uporządkowania na szczeblu międzynarodowym. Miał temu służyć projekt finansowany przez Komisję Europejską (CNET/LUX/2020/OP/0059, 2021-2022), w którym wiodącą rolę pełniła holenderska

organizacja EOKM, zarządzająca także lokalną infolinią Meldpunt Kinderporno. Celem tej inicjatywy było położenie podwalin pod interoperacyjność wzajemnie połączonych na szczeblu unijnym i globalnym zbiorów wartości *hash* przypisanych do CSAM, co powinno dawać lepsze wyniki współpracy między wszystkimi stronami zainteresowanymi ich szybszym i bardziej efektywnym usuwaniem z cyberprzestrzeni. Przygotowanie niniejszego opracowania zbiegło się w czasie z publikacją dwóch raportów, będących wynikiem tego projektu (Publications Office of the European Union, 2022), jak również początkiem kluczowego jak się wydaje przedsięwzięcia dla tej dziedziny, tj. projektu Global Standard (INHOPE, 2023).

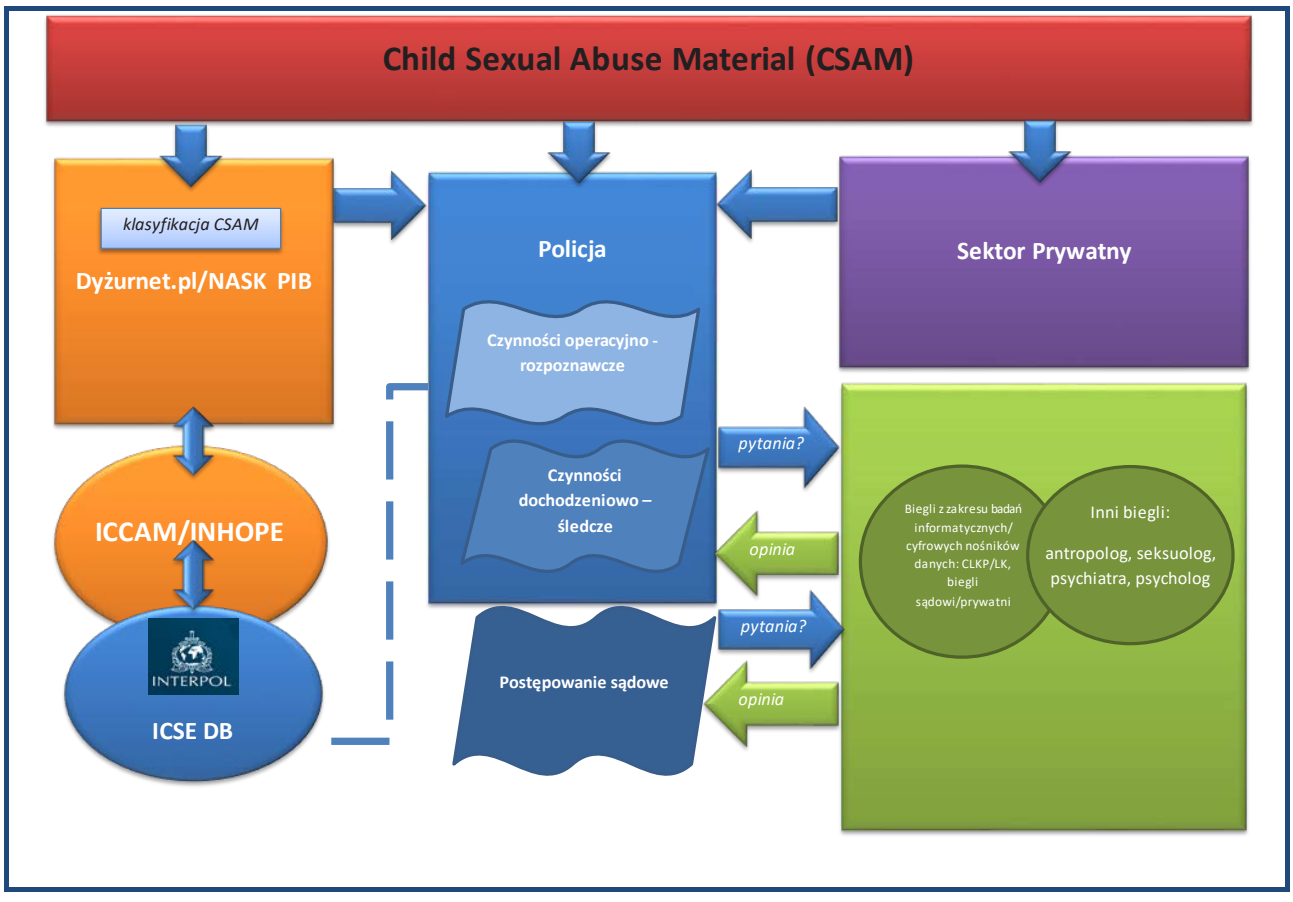
Aktualna sytuacja w Polsce

Analizę aktualnego stanu przedsięwzięć w Polsce należy zacząć od przyjrzenia się temu, jak informacja o treściach z kategorii CSAM jest zagospodarowywana przez działające na arenie krajowej podmioty, mające z nimi do czynienia w ramach wykonywanych obowiązków. Zaliczają się do nich:

- Dyżurnet.pl;
- Policja;
- przedstawiciele środowiska certyfikowanych specjalistów i biegłych;
- przedstawiciele środowiska dostawców produktów i usług internetowych (sektor prywatny).

Zamieszczony poniżej schemat przedstawia istotne elementy procesu zarządzania informacją o CSAM z udziałem wyżej wymienionych podmiotów. Warto już w tym miejscu zaznaczyć, iż obecna komunikacja pomiędzy tymi podmiotami nie pozwala na uniknięcie duplikowania się wysiłków w zakresie przeprowadzanych przez nie badań, czego efektem jest wielokrotne analizowanie tych samych treści. Taka praktyka przekłada się wprost na realne straty w budżecie państwa, z którego finansowana jest działalność podmiotów szczególnie zainteresowanych opisywanymi tu analizami, tj. organów ścigania i wymiaru sprawiedliwości.

Dyżurnet.pl tworzy zespół specjalistów zatrudnionych w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym (dalej: NASK PIB), w ramach działającego od 2005 r. punktu kontaktowego do zgłaszania nielegalnych treści w Internecie. Od 2018 r. działalność tego zespołu została dodatkowo umocowana w Ustawie z dnia 5 lipca 2018 r., o Krajowym Systemie Cyberbezpieczeństwa. Użytkownicy cyberprzestrzeni, którzy spotkali się w tym wymiarze z treściami budzącymi ich niepokój, mogą dokonywać zgłoszeń na kilka sposobów: poprzez formularz znajdujący się na stronie



Ryc. 1. Schemat zarządzania informacją o CSAM w Polsce

internetowej www.dyzurnet.pl, skrzynkę poczty elektronicznej dyzurnet@dyzurnet.pl, automatyczną infolinię 801 615 005, zaś od 2020 r. również przez wtyczkę do przeglądarek Firefox i Chrome.

Treści objęte procedurą reagowania przez Dyżurnet.pl są następujące:

- treści przedstawiające seksualne wykorzystywanie dziecka: art. 202 §3, 4, 4a, 4b Ustawy z dnia 6 czerwca 1997, Kodeks karny, (dalej: k.k.);
- treści przedstawiające tzw. twardą pornografię: art. 202 §3 k.k.;
- treści propagujące rasizm i ksenofobię: art. 256 k.k.;
- inne nielegalne treści, tj. nienależące do żadnej z powyższych kategorii, ale zagrażające bezpieczeństwu dzieci, np. propagowanie lub pochwalanie zachowań o charakterze pedofilskim (art. 200b k.k.), uwodzenie małoletniego poniżej 15 r.ż. przez Internet (art. 200a k.k.), zjawisko szantażu na tle seksualnym (określane również jako ang. *sextortion*), (Dyżurnet, 2021).

W zależności od lokalizacji serwera, na którym znajdują się treści z kategorii CSAM, specjaliści Dyżurnet.pl postępują zgodnie z dwoma scenariuszami. Jeśli takie treści znajdują się na serwerze zlokalizowanym w Polsce albo poza terytorium Polski, ale w kraju, gdzie nie działa infolinia zrzeszona w INHOPE, to informacja o nich jest przekazywana do Komendy Głównej Policji w Warszawie, na adres: cyber-kgp@policja.gov.pl oraz do INTERPOLu. Jeżeli natomiast zgłoszone treści znajdują się na serwerze zlokalizowanym poza terytorium Polski, ale na terenie kraju, w którym działa infolinia zrzeszona w INHOPE, to właśnie do niej i do INTERPOLu trafia stosowna informacja (Dyżurnet.pl, 2021).

W przypadku działania Dyżurnet.pl, powiadomienie INTERPOLu, a w praktyce także przekazanie zdjęć lub filmów drogą cyfrową do ICSE DB, odbywa się za pośrednictwem innej bazy danych, tj. ICCAM (ang. *I see Child Abuse Material*), uruchomionej w 2015 r. dzięki współpracy INHOPE z firmą prywatną Ziuz Forensics oraz finansowaniu z funduszy unijnych. Najistotniejszą cechą tej bazy jest możliwość dokonywania klasyfikacji zgłaszanych treści ze względu na cechy uwiecznionej na nich osoby, takie jak jej płeć oraz przybliżony wiek. W oparciu o tę klasyfikację, z bazy ICCAM trafiają do ICSE DB treści sklasyfikowane jako ang. *baseline*, czyli uznawane za nielegalne we wszystkich państwach współpracujących z INTERPOLem, jak również te sklasyfikowane jako ang. *national*, czyli uznawane za nielegalne w kraju działania infolinii otrzymującej zgłoszenie (INHOPE, 2020). Kryteria klasyfikacji treści w kategorii *baseline* są następujące: zdjęcie lub film powinno bez jakichkolwiek wątpliwości przedstawiać obraz prawdziwego dziecka, w okresie przedpokwitaniowym, czyli przed osiągnięciem 13 r.ż., uczestniczącego lub będącego świadkiem seksualnej aktywności lub być zogniskowane na rejon genitalny lub analny tego dziecka (INHOPE, 2021).

Jeśli zgodnie ze wstępną klasyfikacją analityka infolinii, treści znajdujące się na zgłoszonej stronie internetowej mogą być uznane ze nielegalne, adres URL takiej strony jest przekazywany do bazy ICCAM, gdzie następuje automatyczne przeszukanie wszystkich informacji znajdujących się pod tym adresem, nadanie wartości *hash* każdemu zdjęciu lub filmowi wideo, jak również ustalenie lokalizacji serwera. Wartość *hash* jest następnie porównywana z listami innych wartości *hash* będącymi częścią bazy ICCAM: treści z kategorii *baseline* oraz tych sklasyfikowanych jako nielegalne zarówno w kraju pochodzenia serwera, jak i otrzymującego zgłoszenie. Jeśli wartości *hash* nowo zgłoszonych treści nie pasują do żadnej z tych list, podlegają one indywidualnej klasyfikacji przez analityka, który nadaje im jedną z trzech kategorii: *baseline*, nielegalne w kraju pracy analityka (*national*) lub legalne w tymże kraju. W przypadku Polski, analitycy Dyżurnet.pl posługują się w swoich działaniach podziałem na: treści definiowane jako „treści pornograficzne z udziałem małoletniego" (art. 202 §3, 4, 4a, 4b k.k.) oraz „treści prezentujące dziecko w kontekście seksualnym", takie jak nacechowane seksualnie pozowanie.

Kolejnym podmiotem, który w ramach wykonywania swoich obowiązków ma do czynienia z treściami z kategorii CSAM, jest polska Policja. Dotyczy to różnych obszarów jej działania i związanych z tym działaniem uprawnień: czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych, jak również udziału w postępowaniu przed sądem. Nadrzędnym problemem tej formacji jest jednak ograniczone – w porównaniu do wielu innych, zagranicznych formacji policyjnych – korzystanie z kompetencji służących do identyfikacji dzieci będących ofiarami wykorzystywania seksualnego. Taka identyfikacja ma na celu ustalenie w pierwszej kolejności tożsamości i lokalizacji dziecka, którego wizerunek został utrwalony w materiałach zawierających zapis wizualny czynu zabronionego z jego udziałem, a w następnej potencjalnego sprawcy wykorzystywania seksualnego. Główną przyczyną takiej sytuacji jest brak systemowego podejścia do weryfikacji takich materiałów, sprowadzający się do dostępu do kluczowego dla tego obszaru narzędzia, jakim jest ICSE DB, tylko na poziomie krajowym, za pośrednictwem Komendy Głównej Policji w Warszawie (Wydział dw. z Handlem Ludźmi znajdujący się w strukturach Biura Kryminalnego). Pozostałych przyczyn należy upatrywać w braku możliwości korzystania z innych, opisywanych tu narzędzi: centralnej bazy referencyjnej, zawierającej pliki z kategorii CSAM, jak również nieposiadaniu własnej, wiarygodnej listy wartości *hash*, dotyczących materiałów, które zostały wcześniej sklasyfikowane jako CSAM przez policjantów mających z nimi kontakt w ramach wykonywanych czynności służbowych. Przez „wiarygodną" listę wartości *hash* należy rozumieć listę tworzoną w wyniku procesu opartego na jednolitym systemie klasyfikacji CSAM, uwzględniającym doświadczenia wynikające z wymiany informacji

i szkoleń, mających miejsce zwłaszcza na poziomie międzynarodowym. Często stosowaną tutaj zasadą jest weryfikacja klasyfikacji nadanej CSAM przez trzy osoby, tak aby uzyskać pełną zgodność w ich ocenie.

W Policji funkcjonują ponadto certyfikowani specjaliści[2] oraz biegli[3], o specjalnościach z zakresu badań informatycznych oraz badań cyfrowych nośników danych, zatrudnieni w policyjnych laboratoriach kryminalistycznych, którzy także – w ramach otrzymywanych zleceń i postanowień – mogą stykać się z treściami z kategorii CSAM (Centralne Laboratorium Kryminalistyczne Policji, dalej: CLKP, 2018). Niestety, dokumenty w postaci metodyki badań informatycznych oraz badań cyfrowych nośników danych nie są ogólnie dostępne, przez co zagadnienia z tego obszaru nie mogły zostać ujęte w niniejszym opracowaniu. Jest to niewątpliwie temat na odrębną publikację z udziałem przedstawicieli tego środowiska. W tym miejscu przydatne będzie natomiast przywołanie zakresów czynności certyfikowanego specjalisty oraz biegłego, zatrudnionych w pracowniach cyfrowych nośników danych oraz badań informatycznych, opublikowanych np. przez Laboratorium Kryminalistyczne KWP w Łodzi. Zgodnie z nimi do zakresu czynności certyfikowanego specjalisty zatrudnionego w pracowni cyfrowych nośników danych należy:

- wykonywanie kopii obrazu z zapisów wizualnych;
- rejestracja czynności procesowych;
- wyodrębnienie z zapisów wizualnych kadrów i ich edycja;
- wykonywanie dokumentacji poglądowych;
- zabezpieczanie danych z nośników cyfrowych;
- wykonywanie kopii binarnych nośników cyfrowych;
- odczyt zawartości telefonów komórkowych;
- przeglądanie, wstępna selekcja i konwertowanie plików;
- zabezpieczenie zapisów z cyfrowych rejestratorów obrazu.

Jeśli chodzi o zakres czynności biegłego z tej samej pracowni, to poza ww. czynnościami znajdują się w nim również:

- badania identyfikacyjne utrwalonych obiektów i miejsc na podstawie zapisów wizualnych (odzieży, pojazdów, numerów identyfikacyjnych, logo);
- badania identyfikacyjne urządzeń służących do utrwalania;
- badania zapisów wizualnych pod kątem określenia metod i śladów ingerencji w zarejestrowany obraz;
- badania mające na celu ustalenie wymiarów obiektów w oparciu o utrwalony obraz;
- dokonywanie innych ustaleń możliwych do stwierdzenia w oparciu o analizę zapisu wizualnego (np. selekcja materiału, ustalenie czasu rejestracji obrazu, miejsca rejestracji, sprzętu użytego do rejestracji), (LK KWP w Łodzi, 2022).

W przypadku Pracowni Badań Informatycznych, do typowego zakresu czynności certyfikowanego specjalisty będzie należało:

- zabezpieczanie danych z komputerów, dysków;
- wykonywanie kopii nośników danych;
- zgrywanie zawartości telefonów komórkowych;
- przeglądanie plików i wstępna selekcja;
- konwertowanie.

Z kolei biegły zatrudniony w tej samej pracowni, poza ww. czynnościami będzie wykonywał również:

- badania sprzętu komputerowego i urządzeń peryferyjnych;
- ustalanie przeznaczenia urządzeń informatycznych, ich sprawności oraz zawartości ich pamięci;
- ustalanie i analizę zawartości cyfrowych nośników danych z wyjątkiem:
  - ustalania legalności, wyceny i właścicieli praw autorskich programów, plików dźwiękowych i wideo oraz treści zawartych w plikach tekstowych,
  - ustalania płci i wieku osób zarejestrowanych w plikach oraz charakteru ich treści (np.: pornografia, erotyka, przemoc itp.),
- odzyskiwanie danych z nośników cyfrowych i ich analizę z wyłączeniami wymienionymi w punkcie 3;
- badania telefonów GSM – odczyt danych z pamięci i kart SIM, (LK KWP w Łodzi, 2022).

Łatwo zauważyć, że opisane powyżej czynności są ukierunkowane na dwa obszary: zawartość cyfrowych nośników danych oraz aktywność ich użytkownika, natomiast ich celem jest wypowiedzenie się przez biegłego co do istotnych dla prowadzonego postępowania informacji z tych obszarów. W tym przypadku kluczową obserwacją dla analizowanych w niniejszym opracowaniu zagadnień, dotyczącą tej grupy funkcjonariuszy i pracowników Policji, będzie ta, że ich czynności prowadzone są zatem pod zupełnie innym kątem niż identyfikacja dziecka i sprawcy przestępstwa seksualnego, popełnionego na jego szkodę. Zgodnie z zakresami ich czynności, certyfikowani specjaliści oraz biegli nie powinni się wypowiadać odnośnie płci i wieku osób zarejestrowanych w plikach oraz charakteru ich treści, co jest z kolei podstawą każdej czynności identyfikacyjnej. Wydaje się natomiast, że z racji posiadanych umiejętności osoby te mogłyby tworzyć podwaliny nowej specjalności kryminalistycznej zajmującej się zagadnieniami z zakresu identyfikacji ofiary lub sprawcy, lub też współpracować z utworzonym np. na poziomie centralnym, interdyscyplinarnym zespołem realizującym kompetencje w tym zakresie.

[2] Tytuł certyfikowanego specjalisty uprawnia jego posiadacza do przeprowadzania samodzielnych czynności technicznych, udokumentowanych – w zakresie ich przebiegu i wyników – w sprawozdaniu.

[3] Tytuł biegłego upoważnia natomiast do samodzielnego przeprowadzania czynności technicznych, badań, jak również wnioskowania (art. 200 §2 pkt 5, Ustawy z dnia 6 czerwca 1997, Kodeks postepowania karnego, (dalej: k.p.k) udokumentowanych w sporządzanej opinii, mającej podstawę prawną m.in. w art. 193 k.p.k.

Do problemów dotyczących tej grupy zawodowej, wymagających rozwiązania w pierwszej kolejności, należy ponadto zaliczyć brak komunikacji pomiędzy laboratoriami, skutkujący możliwością wystąpienia sytuacji, kiedy nad plikami o tej samej treści będą pracowali nieświadomi tego faktu policjanci w sąsiadujących ze sobą jednostkach.

Ograniczenia podobnej natury dotyczą również innych biegłych, wypowiadających się co do potencjalnie nielegalnych treści na zlecenie prokuratury lub sądu. Regułą jest interdyscyplinarność kompetencji tych biegłych oraz wykonywanie przez nich obowiązków biegłego na zasadzie dodatkowego zajęcia. Ponadto występujące między biegłymi różnych specjalności różnice kompetencyjne często wymagają dokonywania uzupełniających analiz: przykładem jest tu choćby współpraca biegłego seksuologa i antropologa, w zakresie oceny wieku dziecka uwidocznionego na analizowanych treściach (opinia kompleksowa). Proces oceny treści, co do których ci biegli mają się wypowiedzieć, jest zazwyczaj czasochłonny i w większości przypadków uzależniony od rodzaju materiałów audiowizualnych, tj. zdjęcia vs. filmy wideo, jak również ich ilości oraz zawartości. Obecnie dużym utrudnieniem w pracy tych biegłych jest brak standardów ujednolicających ich funkcjonowanie, zwłaszcza w tak kluczowych kwestiach jak: podejście do ocenianych treści, tj. każde zdjęcie z osobna vs. ogólna ocena treści posiadających określony charakter, dostęp do szkoleń czy też potrzeba posiadania przez nich zapisów wizualnych, mogących zawierać nielegalne treści, na własnym sprzęcie komputerowym.

Ostatnią grupą podmiotów uwzględnionych na schemacie są podmioty zaliczane do tzw. sektora prywatnego, obejmującego dostawców różnego rodzaju produktów i usług internetowych. Realny obraz zaangażowania tych dostawców (zarówno krajowych, jak i zagranicznych), działających na terenie Polski, w przeciwdziałanie dostępności CSAM w ich produktach i usługach jest trudny do nakreślenia. Przede wszystkim w Polsce nie obowiązuje wymóg prawny, tak jak ma to miejsce w Stanach Zjednoczonych, zgodnie z którym dostawcy ci byliby zobligowani do przesyłania zespołowi Dyżurnet.pl raportów dotyczących potencjalnych przypadków ujawnienia CSAM. Stan ten ma jednak szanse ulec znaczącej zmianie w najbliższej przyszłości dzięki przeznaczonym dla tego obszaru inicjatywom na poziomie unijnym. W lipcu 2020 r. została ogłoszona unijna strategia, wzywająca do bardziej efektywnej walki z seksualnym wykorzystywaniem dzieci (Komisja Europejska, 2020), natomiast niedługo potem, w grudniu 2020 r., nowa propozycja legislacyjna w postaci Kodeksu Usług Cyfrowych (Komisja Europejska, 2020). Dla omawianej tu dziedziny kluczowe będą jednak rozwiązania towarzyszące kolejnej propozycji legislacyjnej Komisji Europejskiej, z maja 2022 r., regulującej obowiązki dostawców usług internetowych w obszarze wykrywania, raportowania i usuwania CSAM z ich produktów i usług (Komisja Europejska, 2022). Warto w tym miejscu odnotować, iż niemalże chwilę po jej ogłoszeniu rozpoczęła się globalna dyskusja, dotycząca konieczności wytyczenia granicy pomiędzy działaniami mającymi na celu ochronę dzieci a prawem do prywatności użytkowników tych produktów i usług.

Propozycje rozwiązań mających na celu poprawę obecnej sytuacji na poziomie krajowym

Biorąc pod uwagę rozważania zaprezentowane we wcześniejszych częściach tego opracowania, należy założyć, iż w przypadku Polski istotną poprawę obecnej sytuacji można uzyskać dzięki wdrożeniu systemowych rozwiązań, w ramach których wymienione wcześniej podmioty będą mogły korzystać z dostępnych na rynku rozwiązań technologicznych. Takie podejście jest od dawna promowane przez ekspertów w omawianej dziedzinie (np. WeProtect, 2021).

Przedstawione w dalszej części tego opracowania rozwiązania systemowe na poziomie krajowym zakładają dwutorowe działania, polegające na:

- traktowaniu treści z kategorii CSAM dostępnych w cyberprzestrzeni jako dowodów przestępstwa i nadawaniu im właściwego priorytetu, pozwalającego na dotarcie w pierwszej kolejności do dzieci będących ofiarami wykorzystywania seksualnego w czasie rzeczywistym (rola organów ścigania), oraz
- usuwaniu tego typu treści, nawet historycznych, z cyberprzestrzeni (rola Dyżurnet.pl oraz sektora prywatnego).

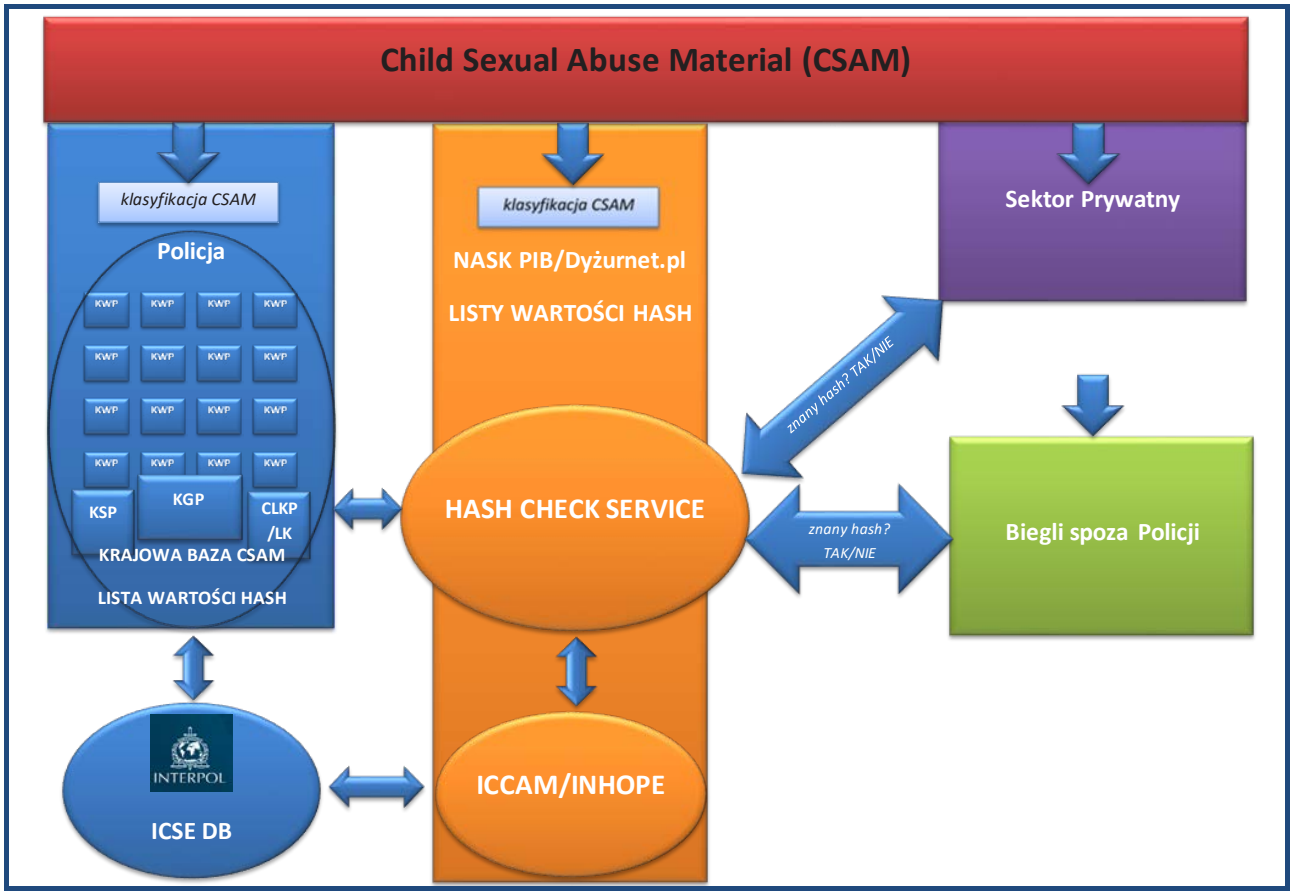
Postulowane tu zmiany systemowe, przedstawione na zamieszczonym poniżej schemacie, opierają się zatem na wdrożeniu stosownych narzędzi na poziomie krajowym: Krajowej Bazy CSAM, tj. bazy materiałów audiowizualnych przedstawiających wykorzystywanie seksualne dzieci, oraz list zawierających wartości *hash* przypisane treściom sklasyfikowanym w wyniku rzetelnego procesu jako CSAM. Za kluczowy element tych zmian należy uznać umożliwienie komunikacji pomiędzy funkcjonującymi w Polsce podmiotami, mającymi dostęp do CSAM w ramach wykonywanych obowiązków. Taką funkcjonalność oferuje np. rozwiązanie w postaci ang. *Hash Check Service* (dalej: HCS), wdrażane od 2019 r. w Holandii i aktualnie przekształcane w bardziej zaawansowaną postać, określaną jako ang. *Instant Image Identifier* (EOKM, 2022). W dużym uproszczeniu, rozwiązanie to umożliwia upoważnionym do tego podmiotom przesłanie zapytania, czy posiadany przez nie plik to wcześniej sklasyfikowany CSAM. Taka komunikacja, wykorzystująca protokół sieci www – HTTPS, odbywa się bez konieczności przesyłania właściwego pliku – nadana mu wartość *hash* porównywana jest za pomocą dedykowanego interfejsu API z zawartością zbioru takich wartości, będących w zarządzie wymienionej już tutaj wcześniej holenderskiej organizacji EOKM.

W zależności od wyników sprawdzenia podmiot przesyłający zapytanie otrzymuje odpowiedź twierdzącą lub przeczącą.

Postulowane tutaj rozwiązania obejmują w pierwszej kolejności Policję, w której zasobach powinna się znaleźć Krajowa Baza CSAM, umożliwiająca komunikację z jednostkami terenowymi tej formacji, gdzie trafiałyby materiały zabezpieczone w związku z prowadzonymi na terenie Polski postępowaniami. Koronnym argumentem przeciwko zarzutowi, iż byłoby to duplikowanie bazy danych ICSE, jest możliwość tworzenia przez Policję własnej listy wartości *hash*, zasilanej obowiązkowo za każdym razem ujawnienia i sklasyfikowania treści z tej kategorii w ramach prowadzonych czynności. Takie postępowanie miałoby bezpośredni wpływ na zwiększenie efektywności tej służby w omawianym tutaj obszarze. Ponadto kompetencja identyfikacji dzieci – ofiar wykorzystywania seksualnego, powinna objąć specjalnie do tego powołane zespoły w jednostkach terenowych Policji, realizujące czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze, stąd postulowaną w tym obszarze zmianą jest umożliwienie dostępu do ICSE DB jednostkom terenowym Policji, tj. na szczeblu każdego województwa, w tym komendy stołecznej.

Policyjna lista wartości *hash* (tylko lista, nie właściwe pliki lub ich kopie) byłaby udostępniana NASK PIB, a w praktyce zespołowi Dyżurnet.pl, odpowiedzialnemu za funkcjonowanie HCS w polskich warunkach. Zadaniem Dyżurnet.pl byłoby zarządzanie zgromadzonymi listami: własną, na którą trafiałyby cyfrowe podpisy plików, o których zespół Dyżurnet.pl został powiadomiony za pośrednictwem przeznaczonych do tego kanałów lub w ramach współpracy z sektorem prywatnym, listą policyjną, jak również listami pozyskanymi od wiarygodnych partnerów, takich jak INTERPOL, Europol, NCMEC czy IWF. Warto dodać, że podobne starania w tym obszarze zostały w przeszłości podjęte przez NASK PIB, dzięki uruchomieniu aplikacji SYWENTO. Wspomaga ona analizę danych przez biegłych z zakresu informatyki pod kątem uzyskania informacji, czy pod danym adresem internetowym (URL) znajdowały się treści pornograficzne z udziałem małoletniego. Zapytanie skierowane do aplikacji SYWENTO generuje informację zwrotną, czy adresy URL wprowadzone do systemu przez biegłego występują w bazie adresów zidentyfikowanych przez Dyżurnet.pl (Dyżurnet.pl, 2022).

Oprócz wyposażenia funkcjonariuszy Policji w narzędzia technologiczne, osoby pełniące służbę



Ryc. 2. Propozycja wdrożenia rozwiązań opartych na wymianie wartości *hash* w Polsce

w przeznaczonych do zwalczania wykorzystywania seksualnego dzieci zespołach powinny zostać objęte obowiązkowym, specjalistycznym szkoleniem, obejmującym charakterystykę zjawiska wykorzystywania seksualnego dzieci, techniki przesłuchania sprawców i ofiar, jak również sposoby radzenia sobie z konsekwencjami kontaktu z tak szczególnym rodzajem przestępczości, w tym koniecznością klasyfikacji CSAM. Zasadnym wydaje się również wzbogacenie wachlarza kompetencji policyjnych psychologów, tak aby mogli oni świadczyć systemową i proaktywną pomoc swoim kolegom i koleżankom, mierzącym się w swojej pracy z jednym z najtrudniejszych wyzwań, jakim jest obcowanie z materiałami przedstawiającymi wykorzystywane seksualnie dzieci.

Możliwość przesyłania zapytań do HCS byłaby szczególnie pomocna dla przedstawicieli podmiotów sektora prywatnego w Polsce, którzy w ten sposób mogliby weryfikować treści występujące w ich produktach i usługach bez ponoszenia kosztów związanych z indywidualnym wdrożeniem takich rozwiązań, w tym zatrudnieniem i wyszkoleniem moderatorów treści. Mając na uwadze zmiany, które ma spowodować pakiet unijnych propozycji legislacyjnych w tym obszarze, taką usługą powinny być szczególnie zainteresowane podmioty sektora prywatnego małej i średniej wielkości, w przypadku których zastosowanie się do nowych regulacji może stanowić poważne obciążenie finansowe.

W grupie podmiotów mogących odnieść korzyści z funkcjonowania HCS znaleźliby się również biegli funkcjonujący poza Policją, w przypadku których możliwość dokonywania zapytań przyczyniłaby się do podniesienia efektywności ich pracy, jak również nadania jej pewnej formy standaryzacji.

Podsumowanie

Cyberprzestrzeń to obecnie miejsce, gdzie dzieci są uwodzone, zastraszane, a nawet szantażowane, w celu uzyskania seksualnie nacechowanych treści z ich udziałem, co przekłada się bezpośrednio na zatrważającą ilość takich treści dostępnych w tym wymiarze. Przedstawiciele Europolu mówią wprost o poważnych konsekwencjach wzrastającej z roku na rok ilości CSAM ujawnionych w cyberprzestrzeni, dla możliwości wykrywczych organów ścigania na całym świecie (Europol, 2020). W obliczu takich wyzwań postulaty nawołujące do wykorzystywania dostępnych technologii są zatem szczególnie aktualne.

Pewne wysiłki zmierzające do zmiany obecnej sytuacji w Polsce zostały podjęte w ramach projektu Komendy Głównej Policji oraz CLKP pod nazwą „Budowa centralnego systemu informacji o plikach związanych z działalnością przestępczą", finansowanego w latach 2014-2020 w ramach unijnego funduszu Bezpieczeństwa Wewnętrznego (Policja, 2020), którego celem była budowa zintegrowanego, centralnego systemu informacji o plikach (haszach) związanych z działalnością przestępczą, zwanego Centralnym Systemem Haszy. Szczegółowymi informacjami na ten temat dysponuje CLKP, jako instytucja sprawująca merytoryczny nadzór nad projektem. Należy założyć, że nabyte w ramach tego projektu doświadczenia będą mogły zostać wykorzystane na potrzeby wdrażania postulowanych w tym opracowaniu, systemowych rozwiązań na poziomie krajowym. Niewątpliwie kluczowym elementem będzie w tym przypadku kompatybilność wykorzystanego w tym projekcie systemu klasyfikacji plików związanych z działalnością przestępczą z systemem, jakim w praktyce posługują się specjaliści zatrudnieni w Dyżurnet.pl, szkoleni m.in. przez INTERPOL.

Inną okazją do zmiany sytuacji krajowej było złożenie przez NASK PIB w lutym 2021 r. propozycji projektu NETTO (ang. *Networking Enhanced Through Technological Opportunities*), o wartości ok. 1 miliona euro, w ramach unijnego Funduszu Bezpieczeństwa Wewnętrznego. Propozycja ta, pomimo uzyskania wysokiej oceny w konkursie projektów, nie otrzymała ostatecznie dofinansowania, co nie przesądziło o ponownym wykorzystaniu zawartej w niej koncepcji w kolejnym projekcie NASK PIB, zgłoszonym do konkursu rok później.

Nadzieję na zmianę odpowiedzi krajowej na problem wykorzystywania seksualnego dzieci można obecnie pokładać w dwóch niedawnych, znaczących dla omawianego tu obszaru inicjatywach. Pierwszą z nich jest powołanie Zarządzeniem Ministra Sprawiedliwości z dnia 29 września 2021 r. Zespołu do spraw przeciwdziałania przestępczości przeciwko wolności seksualnej i obyczajności na szkodę osób małoletnich (Ministerstwo Sprawiedliwości, 2021). Drugą inicjatywą jest natomiast powołanie w Policji, od 12 stycznia 2022 r., Centralnego Biura Zwalczania Cyberprzestępczości (Policja, 2021). W tym przypadku kluczowe wydaje się przyjęcie założenia, że zjawisko wykorzystywania seksualnego dzieci w cyberprzestrzeni zalicza się do kategorii cyberprzestępczości. Założenie to powinno znaleźć odzwierciedlenie w decyzjach określających organizację i kompetencje nowo powołanego Biura.

Źródła rycin: autor

Bibliografia

1. Canadian Centre for Child Protection, (2017). Survivors' survey. Pobrano z: https://www.protectchildren.ca/en/resources-research/survivors-survey-results/ (dostęp: 27 stycznia 2022).
2. Centralne Laboratorium Kryminalistyczne Policji, (2017). Badania informatyczne. Pobrano z: https://clkp.policja.pl/clk/badania-i-projekty/langnodata/badania-informatyczne/153011,Badania-Informatyczne.html (dostęp: 21 marca 2022).

3. Centralne Laboratorium Kryminalistyczne Policji, (2017). Decyzja nr 164 Dyrektora CLKP z dnia 29.06.2018 r. w sprawie wykazu specjalności kryminalistycznych, w zakresie których wydawane są opinie i sprawozdania z czynności przeprowadzonych w policyjnych laboratoriach kryminalistycznych.
4. Centralne Laboratorium Kryminalistyczne Policji, (2018). Decyzja nr 166 Dyrektora CLKP z dnia 29.06.2018 r. w sprawie typowych zakresów czynności biegłego i specjalisty w specjalnościach kryminalistycznych.
5. Child Rescue Coalition, (2021). Pobrano z: https://childrescuecoalition.org/the-issue/ (dostęp: 11 października 2021).
6. Cybertip!ca, (2022). Pobrano z: https://www.cybertip.ca/en/child-sexual-abuse/project-arachnid/ (dostęp: 30 maja 2022).
7. Dyżurnet.pl, (2021). Raport Dyżurnet.pl 2020. Pobrano z: https://dyzurnet.pl/publikacje (dostęp: 11 października 2021).
8. Dyżurnet.pl, (2022). Pobrano z: https://dyzurnet.pl/dla-profesjonalistow/wpis/sywento (dostęp: 30 maja 2022).
9. Elshenraki, H.N. (2021), Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities. *Advances in Criminology, Criminal Justice, and Penology*.
10. EOKM, (2022). Pobrano z: https://www.3-is.eu/#objectives oraz https://www.3-is.eu/sites/default/files/2022-05/iii-description-tool-v2_0.pdf (dostęp: 30 maja 2022).
11. Europol, (2015). Pobrano z: https://www.europol.europa.eu/sites/default/files/documents/efc_strategic_assessment__public_version.pdf (dostęp: 16 maja 2022).
12. Europol, (2017). Pobrano z: https://www.europol.europa.eu/newsroom/news/14-arrests-in-take-down-of-massive-child-sexual-abuse-platform oraz https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe (dostęp: 11 października 2021).
13. Europol, (2020). Internet Organised Crime Threat Assessment. Pobrano z: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (dostęp: 11 października 2021).
14. Europol, (2021). Internet Organised Crime Threat Assessment. Pobrano z: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021 (dostęp: 3 lutego 2022).
15. Gazeta Policyjna, (2021). Numer 2 Specjalny. Pobrano z: https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s (dostęp: 27 stycznia 2022).
16. INHOPE, (2020). Annual report 2020. Pobrano z: https://inhope.org/media/pages/the-facts/download-our-whitepapers/annual-report/bb4dd3cdc3-1628156678/inhope-annual-report-2020.pdf (dostęp: 12 października 2021).
17. INHOPE, (2021). Pobrano z: https://www.inhope.org/EN, https://inhope.org/EN/articles/what-is-baseline (dostęp: 11 października 2021).
18. INHOPE, (2022). Pobrano z: https://inhope.org/EN/articles/the-global-standard-project (dostęp: 21 listopada 2021).
19. Internet Watch Foundation, (2022). Pobrano z: https://www.iwf.org.uk/our-technology/intelligrade/ oraz https://www.iwf.org.uk/our-technology/crawler/ (dostęp: 30 maja 2022).
20. INTERPOL, (2022). Pobrano z: https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database (dostęp: 21 listopada 2022).
21. Komisja Europejska, (2020). 'EU strategy for a more effective fight against child sexual abuse'. Pobrano z: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agendasecurity/20200724_com-2020--607-commission-communication_en.pdf (dostęp: 3 lutego 2022).
22. Komisja Europejska, (2020). Networks, Content and Technology, *Study on framework of best practices to tackle child sexual abuse material online : executive summary (English)*, Publications Office, 2020, https://data.europa.eu/doi/10.2759/386477.
23. Komisja Europejska, (2020). Kodeks Usług Cyfrowych. Pobrano z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_pl (dostęp: 30 lutego 2022).
24. Komisja Europejska, (2022). Pobrano z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472 (dostęp: 30 maja 2022).
25. Laboratorium Kryminalistyczne KWP w Łodzi. Pobrano z: https://lk-lodzka.policja.gov.pl/el8/struktura/sekcja-dokumentow/pracownia-cyfrowych-nos/606,Pracownia-Cyfrowych-Nosnikow-Danych.html oraz https://lk-lodzka.policja.gov.pl/el8/struktura/sekcja-dokumentow/pracownia-badan-informa/604,Pracownia-Badan-Informatycznych.html (dostęp: 11 lipca 2022).
26. Lee, H-E., Ermakova, T., Ververis, V., Fabian, B. (2020). Detecting child abuse material: A comprehensive survey. Forensic Science International: Digital Investigation, *34*. http://doi.org/10.1016/j.fsidi.2020.301022.
27. Microsoft, (2020). Pobrano z: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/ (dostęp: 21 listopada 2022).

28. National Center for Missing & Exploited Children, (2020). Pobrano z: https://www.missingkids.org/gethelpnow/cybertipline (dostęp: 8 września 2021).
29. National Center for Missing & Exploited Children, (2020). Pobrano z: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata (dostęp: 28 kwietnia 2022).
30. Policja, (2020). Pobrano z: https://clkp.policja.pl/clk/badania-i-projekty/fundusz-bezpieczenstwa/153261,Fundusz-Bezpieczenstwa-Wewnetrznego.html (dostęp: 8 września 2021).
31. Publications Office of the European Union, (2022). Pobrano z: https://op.europa.eu/en/publication-detail/-/publication/986ca706-cce4-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257046699 oraz https://op.europa.eu/en/publication-detail/-/publication/3e8e564c-cce7-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257046650 (dostęp: 14 czerwca 2022).
32. Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum, 21*, 429-447. http://doi.org/10.1007/s12027-020-00625-7.
33. Rada Europy, (2021). Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse. Pobrano z: https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee (dostęp: 11 października 2021).
34. Seto, M.C., Hanson, R.K., Babchishin, K.C. (2010). Contact Sexual Offending by Men With Online Sexual Offenses. *Sexual Abuse: A Journal of Research and Treatment*, *23*(1), 124-145. http://doi.org/10.1177/1079063210369013.
35. Ustawa z dnia 5 lipca 2018 r., o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2020 r., poz. 1369 t.j. z późn. zm.).
36. Ustawa z dnia 6 czerwca 1997 r., Kodeks karny (Dz.U. 2021 r., poz. 2345 t.j. z późn. zm.).
37. Ustawa z dnia 6 czerwca 1997 r., Kodeks postepowania karnego (Dz.U. 2021, poz. 534 t.j. z późn. zm.).
38. Ustawa z dnia 17 grudnia 2021 r., o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. 2021, poz. 2447).
39. Wasilewski, J. (2013). Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego*, *9*, 225-234.
40. WeProtect, (2021). The Model National Response. Pobrano z: https://www.weprotect.org/model-national-response/ (dostęp: 3 lutego 2022).
41. Web-IQ, (2020). EU Strategy proposal CSAM lifecycle and interception. Pobrano z: https://vimeo.com/434684287 (dostęp: 8 września 2021).
42. Zarządzenie Ministra Sprawiedliwości z dnia 29 września 2021 r. w sprawie powołania Zespołu do spraw przeciwdziałania przestępczości przeciwko wolności seksualnej i obyczajności na szkodę osób małoletnich. Pobrano z: https://www.gov.pl/web/sprawiedliwosc/du-21-233 (dostęp: 3 lutego 2022).

National concept for systemic solutions to combat child sexual exploitation and abuse

Junior Inspector (Ret.) Katarzyna Staciwa, M.A.[1]

[1] NASK - National Research Institute, Department of Response to Illegal Content on the Internet, Dyżurnet.pl, katarzyna.staciwa@nask.pl, ORCID: 0000-0003-0633-4696

Summary

Sexual exploitation and abuse of children in cyberspace, including the presence of content that is a visual record of criminal acts committed against them, is a global problem. The fight against this problem is effective when the actors involved make systemic use of the available technological solutions. This applies in particular to solutions that allow for a quick verification of whether potentially illegal content has been previously classified as Child Sexual Abuse Material (hereinafter: CSAM), as well as to communication between persons accessing such content in the course of their duties.

This study aims to provide an overview of solutions and tools used in this area, both internationally and nationally, and to propose a systemic approach that will contribute to the effectiveness of current solutions in the above area at national level.

Key words: child sexual abuse, child sexual exploitation, cyberspace, Child Sexual Abuse Material, CSAM, hash values

Introduction

The expansion of the Internet computer network in recent years, as well as the increasing number of mobile devices communicating with it, has undoubtedly had an impact on many areas of life in today's society, which is not without reason described as a global village. Technological progress, now an integral part of our lives, has caused that many phenomena occurring in the real world have moved into cyberspace. As J. Wasilewski aptly notes, the essence of the latter "is formed by the concept of bringing to life a kind of parallel environment, which is a new dimension for human activities" (2013). The trend indicated here also applies to the phenomenon of child sexual exploitation and abuse, where the actual behaviour is captured in photographs and videos, which are then distributed digitally between recipients who fall into a particular category of cyberspace users.

The offline and online dimensions have been linked in a particular way. This link has been described in research, for example, by Seto, Hanson and Babchishin (2010), indicating that about 55% of perpetrators operating in the virtual world admitted to sexual abuse of children in reality, and 12% of such perpetrators had a previous criminal record in connection with so-called contact crimes. In contrast, the American non-profit organisation, Child Rescue Coalition (hereafter: CRC), known for providing technological solutions to support law enforcement, indicates the percentage of so-called contact perpetrators in the group of perpetrators operating in the virtual world at 85% (2021).

To illustrate the scale of this phenomenon, it is worth recalling here the facts of the darknet platforms shut down as a result of international law enforcement operations in 2017.[1] These platforms brought together individuals with a sexual interest in children, enabling them to communicate directly, including the distribution of CSAM and the transmission of child sexual exploitation and/or abuse in real time, characterised by a high degree of anonymity. According to information provided by the European Cybercrime Centre (hereafter: EC3), operating within the structures of the European Union Agency for Law Enforcement Cooperation based in the Hague (hereafter: Europol), these platforms ranged from tens of thousands (Elysium platform, over 87,000 users) to even several hundred thousand of users (Playpen platform, over 150,000), (2017).

Information on current trends regarding the phenomenon of child sexual exploitation and abuse in cyberspace can be obtained from reports published by agencies and organisations specialised in this field,

[1] Dark web - is, in simple terms, a hidden part of the Internet resources that can be browsed using special software. The Darknet, on the other hand, is a restricted access network consisting of many distributed, anonymous nodes (such as Tor, I2P or Freenet) that allow access to the dark web.

such as Europol, (2020 and 2021) or the Council of Europe (2021). In these reports, one can observe a breakdown of trends into:

- trends concerning the content of CSAM category and
- trends concerning behaviour in cyberspace (e.g. grooming, solicitation or sexual blackmail).

The results of the analysis of these trends give rise to the conclusion that the phenomenon of child sexual exploitation and abuse will never be completely eliminated from cyberspace, but efforts can and should be made to reduce its scope and scale, although this task too is undoubtedly already a huge challenge. For the most part, these efforts are being made through the use of solutions to quickly verify whether potentially illegal content has already been classified as CSAM, as well as through communication between persons accessing such content in the course of their duties. It should also be noted that attempts are being made to implement solutions using artificial intelligence to identify dangerous online behaviour towards children, such as grooming (Microsoft, 2020). This study takes a closer look - based on the method of analysis and review of literature - at the functioning of solutions referring to the first of the above-mentioned trends, as well as proposes a systemic approach that could improve the effectiveness of current solutions in this area in Poland.

CSAM as a current challenge

The discussion of the first trend mentioned above should start with the thesis that the demand for the availability of child sexual exploitation and abuse content in cyberspace exists i.e. when the users in cyberspace are sexually interested in children persons, especially those who have conditions to commit sexual offences and record them on video. While it is beyond the scope of this paper to provide a full characteristics of such individuals, it is worth noting here that their possession of a new CSAM photograph or video, previously unpublished anywhere else, is a kind of trophy and currency for them (Europol, 2015). The use of the latter can, for example, make it possible to 'move up' in the hierarchy of covert forums on the Internet or gain access to private groups that disseminate, including by live streaming, strictly defined content, often depicting the most brutal and sadistic treatment of a sexually exploited and/or abused child.

It is impossible to estimate how much CSAM is currently available in cyberspace. In its recent publications, Europol once again points to a sustained year-on-year increase in the amount of CSAM content revealed in cyberspace, which naturally translates into its continued distribution and redistribution (Europol, 2020). As estimated by other experts in this field, a single image or video depicting the sexual exploitation and/or abuse of a child can be viewed or shared online up to 70,000 times (Web-IQ, 2020). A figure in excess of 2.5 million can provide another benchmark in efforts to determine the scale of the problem - this refers to IP addresses that have been linked to one of the most commonly shared CSAM category files in cyberspace (CRC, 2021).

An organisation with a special mandate to prevent and combat child sexual exploitation and abuse is the National Center for Missing & Exploited Children in the United States (hereafter: NCMEC). It has within its resources the CyberTipline, i.e. a hotline which is affiliated - like the other 50 hotlines operating in different parts of the world - to the INHOPE association (INHOPE, 2021). Under US federal law, local private sector entities are required to report to CyberTipline incidents of content in their resources that may depict child sexual abuse. This is a unique regulation, with no equivalent anywhere else in the world to date. The figures published by the organisation are alarming: in 2020 CyberTipline received more than 21.7 million such reports, a 28% increase compared to 2019 (2020). In 2021, there was another increase in the number of reports - to 29.3 million (up 35% from 2020), (NCMEC, 2022).

The description of a challenge posed by the presence of CSAM in cyberspace should be concluded by recalling the perspective of the victims of a crime in this category. Studies conducted with these individuals have repeatedly shown that the digital distribution of CSAM exacerbates their victimisation and has a long-term detrimental impact on them even when they reach adulthood (e.g. Canadian Centre for Child Protection, 2017). According to the Centre's survey, 70% of this population are constantly afraid of being recognised in real life. It is therefore the responsibility of the society in which children grow up not only to protect them from sexual exploitation and/or abuse in the real world, but also from experiencing secondary victimisation caused by availability in the virtual world of evidence of an offence committed against them.

Technology on duty

Verification of potentially illegal content by comparing *hash* values assigned to it is nothing new. The use of this method in preventing and combating child sexual exploitation and abuse has already been subject of numerous scientific (e.g. Quayle, 2020; Lee, Ermakova, Ververis, Fabian, 2020; Elshenraki, 2021) as well as expert (e.g. European Commission, 2020; Council of Europe, 2021) publications. This study draws on content from such publications, focusing on the practical side of using this method as a key element in a systemic approach that could be implemented at national level in Poland.

An in-depth analysis of the processes involved in assigning a *hash* value is not the purpose of this paper. At this point, however, it will be useful to clarify that such a value is nothing more than a sequence of digits and characters calculated using various

algorithms (e.g. MD5, SHA-1, PhotoDNA, pHash, TMK PDQF, SIFT), (e.g. Staciwa, 2021; Council of Europe, 2021), so more precise definitions would be the value of a one-way encryption function or the value of a cryptographic hash function (CHF). Since a *hash* value is unique for each file, it is equally often referred to as a 'digital fingerprint'.

The use of the method described here is extremely valuable for all actors involved in identifying child victims of sexual exploitatioin and abuse and combating the availability of CSAM in cyberspace. It is through this method that it is possible to quickly determine whether there is CSAM content in a large collection of digital material. This verification method is the basis for the operation of a special database held by the INTERPOL International Criminal Police Organisation with its headquarters in Lyon (the International Child Sexual Exploitation Database, hereinafter: ICSE DB). The ICSE DB is primarily a platform that enables investigators from more than 68 countries around the world to share criminal intelligence information about their cases. Transfer of content to the ICSE DB makes it possible to verify whether such content has already been identified in another country, as well as whether it bears similarities to other content already in the database, which as of today numbers more than 4.3 million images and videos (INTERPOL, 2022). Verification described here is invaluable for investigators, as it means being able to determine whether the material they are dealing with is new, which justifies the suspicion of real-time sexual exploitation and/or abuse of a child and involves prioritising such a case. Part of the ICSE DB is software that compares images and video so that investigators can establish links between victims, perpetrators and crime scenes in real time. The fact that cooperation of the international investigative community since the inception of ICSE DB has led to identification of 32 700 children worldwide should be an argument for the validity of solutions discussed here (INTERPOL, 2023).

An additional benefit of the classification described here is that a person dealing with potentially illegal content will not have to look again at content that has already been classified, which in practice amounts not only to avoiding duplication of work for those dealing with such content, but also to reducing the amount of time they are exposed to it. Exposure to such special content is highly stressful and, in the interests of the mental and physical well-being of such persons, contact with it should be kept to a minimum.

The creation of reliable lists of *hash* values attributed to CSAM category content and the exchange of information about these values are an invaluable contribution to the efforts of the international community involved in countering the availability of CSAM in cyberspace. The knowledge and experience of those dealing with this type of content as part of their duties, acquired, among other things, in training courses organised by INTERPOL, as well as the possibility to cooperate with other actors at a global level, are elements that enhance the effectiveness of these efforts.

It is worth mentioning at this point that solutions based on the technology described here have long been used by some law enforcement agencies, especially those with national CSAM databases, such as those in Sweden or the UK, as well as those that cooperate on a daily basis within the ICSE DB. The list of entities that use *hash* values in their daily work is further supplemented by some of the hotlines involved in removing illegal content from cyberspace: CyberTipline - United States, Cybertip!ca - Canada, Internet Watch Foundation (hereafter: IWF) - United Kingdom and, more recently, also Meldpunt Kinderporno - the Netherlands. It is these entities, moreover, that are taking steps to maximise the potential of knowledge of pre-classified CSAM content. In the case of the IWF, the IntelliGrade and IWF Crawler projects (IWF, 2022) should be mentioned, while with regard to its Canadian counterpart, Cybertip!ca, it will be the Arachnid project (Cybertip!ca, 2022). What these projects have in common is the desire to classify as much content as possible in order to make the reference databases of *hash* values as complete as possible.

The use of *hash* values is a solution with many benefits, but this area also needs to be sorted out at international level. This was the aim of a project funded by the European Commission (CNET/LUX/2020/OP/0059, 2021-2022), in which the Dutch organisation EOKM, which also manages the local Meldpunt Kinderporno hotline, took the lead. The aim of this initiative was to lay the foundations for the interoperability of interconnected EU- and global-level sets of *hash* values attributed to CSAM content, which should yield better cooperation between all parties interested in their faster and more efficient removal from cyberspace. The preparation of this paper coincided with the publication of two reports resulting from this project (Publications Office of the European Union, 2022), as well as the start of what appears to be a key undertaking in this field, the Global Standard Project (INHOPE, 2022).

Current situation in Poland

The analysis of current state of undertakings in Poland should begin with a look at how information on CSAM content is managed by national actors dealing with it as part of their duties. These include:

- Dyżurnet.pl;
- the Police;
- representatives of the community of certified specialists and experts;
- representatives of the Internet product and service provider community (private sector).

The diagram below shows the essential elements of the CSAM information management process involving the above-mentioned actors. It is worth pointing out that the current communication between these actors

does not avoid duplication of effort in the research they carry out, resulting in multiple analyses of the same content. Such a practice translates directly into real losses in the state budget, from which the activities of the entities particularly interested in the analyses described here, i.e. law enforcement agencies and the judiciary, are financed.

Dyżurnet.pl is formed by a team of specialists employed at the Research and Academic Computer Network - National Research Institute (hereinafter: NASK), as part of the contact point for reporting illegal content on the Internet, which was established in 2005. As of 2018, the activities of this team were further facilitated by the Act of 5 July 2018 on the National Cyber Security System. Users of cyberspace who have encountered content of concern in this respect can report it in several ways: via the form on the website www.dyzurnet.pl, the e-mail box dyzurnet@dyzurnet.pl, the automated hotline 801 615 005, and, from 2020, also via a plug-in for the Firefox and Chrome browsers.

The content covered by the Dyżurnet.pl response procedure is as follows:

- content depicting the sexual exploitation and abuse of a child: article 202 §3, 4, 4a, 4b of the Act of 6 June 1997, the Penal Code;
- content depicting so-called hard pornography: article 202 §3 of the Penal Code;
- content propagating racism and xenophobia: Article 256 of the Penal Code.;
- other illegal content, i.e. content that does not fall into any of the above categories but endangers the safety of children, e.g. promoting or endorsing paedophilic behaviour (Article 200b of the Penal Code), grooming a minor under 15 years of age via the Internet (Article 200a of the Penal Code), sexual blackmail (also known as sextortion), (Dyżurnet, 2021).

Depending on the location of the server on which the CSAM content is stored, Dyżurnet.pl specialists follow two scenarios. If such content is stored on a server located in Poland or outside Poland, but in a country where an INHOPE-affiliated helpline does not operate, information about it is forwarded to the Police Headquarters in Warsaw, at the following address: cyber-kgp@policja.gov.pl and to INTERPOL. If, however, the reported content is located on a server outside Poland, but in a country where an INHOPE-affiliated helpline operates, it is this helpline and INTERPOL that receive the relevant information. (Dyżurnet.pl, 2021).

In the case of the Dyżurnet.pl operation, INTERPOL is notified, and in practice the images or videos are digitally transmitted to the ICSE DB, through another database, i.e. ICCAM (*I See Child Abuse Material*), launched in 2015 thanks to the cooperation of

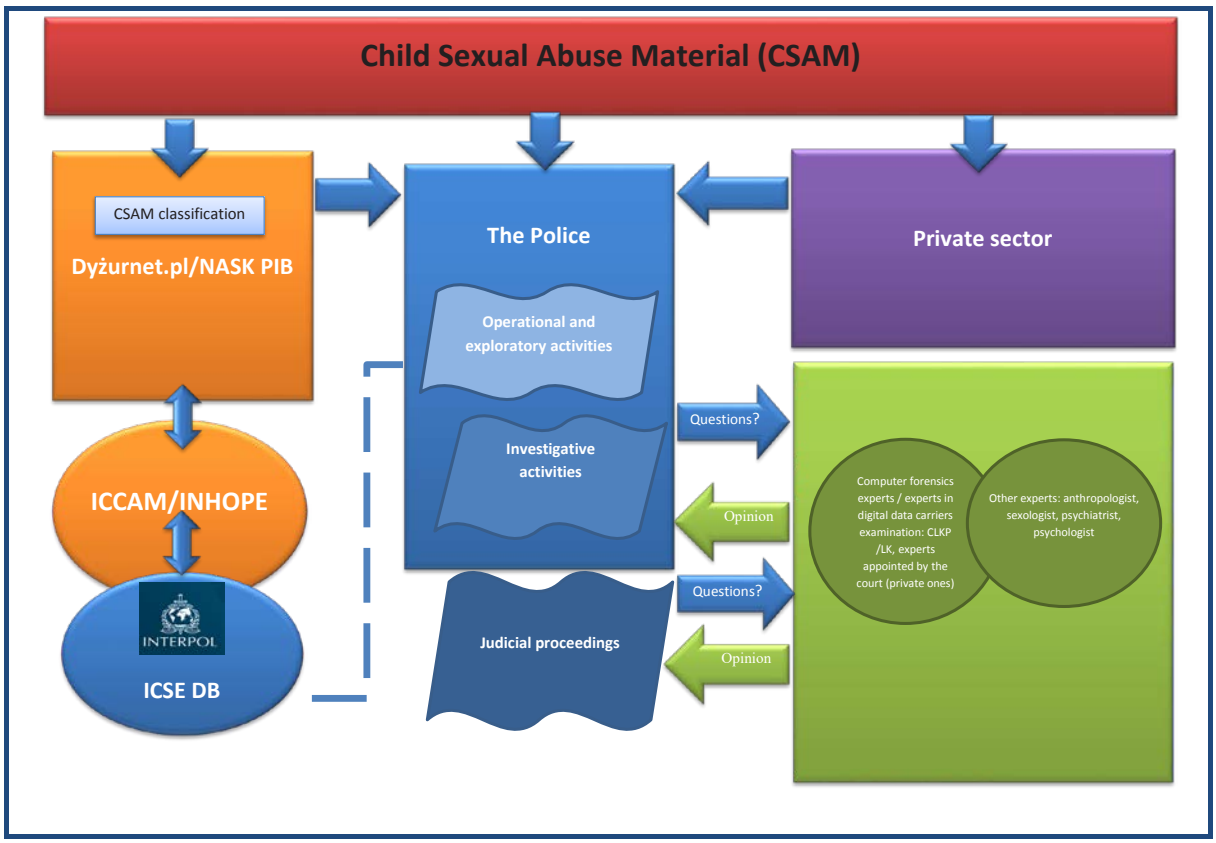


Fig. 1. Diagram concerning the management of information on CSAM in Poland

INHOPE with the private company Ziuz Forensics and EU funding. The most salient feature of this database is the possibility to classify the reported content according to the characteristics of the person pictured on it, such as their gender and approximate age. Based on this classification, content classified as *baseline*, i.e. considered illegal in all INTERPOL cooperating countries, as well as content classified as *national*, i.e. considered illegal in the country of operation of the hotline receiving the call, is submitted to the ICSE DB from the ICCAM database (INHOPE, 2020). The criteria for classifying content in the *baseline* category are as follows: a photo or video should show, without any doubt, an image of a real pre-pubertal child, i.e. before the age of 13, participating in or witnessing sexual activity or should be focused on the genital or anal area of that child (INHOPE, 2021).

If, according to the hotline analyst's initial classification, the content on the reported website can be considered illegal, the URL of such a website is forwarded to the ICCAM database, where an automatic search is performed on all the information at this address, assigning a *hash* value to each photo or video, as well as determining the location of the server. The *hash* value is then compared with lists of other *hash* values that are part of the ICCAM database: content from the *baseline* category and those classified as illegal in both the country of origin of the server and the country receiving the notification. If the *hash* values of newly reported content do not match any of these lists, they are individually classified by the analyst, who assigns them one of three categories: *baseline*, illegal in the analyst's country of work (*national*) or legal in that country. In the case of Poland, Dyżurnet.pl analysts use a distinction between: content defined as 'pornographic content with the participation of a minor' (Article 202 §3, 4, 4a, 4b of the Criminal Code) and 'content presenting a child in a sexual context', such as sexually oriented posing.

The Polish Police is another entity that deals with CSAM content as part of their duties. This applies to various areas of their activities and related powers: operational and exploratory activities, investigative activities, as well as participation in court proceedings. However, the overriding problem of this formation is the limited - in comparison to many other, foreign police formations - use of powers to identify child victims of sexual exploitation and/or abuse. Such identification is aimed at determining, first, the identity and location of a child whose image has been recorded in materials containing a visual recording of a criminal act with his/her participation, and second, a potential perpetrator of sexual exploitation and/or abuse. The main reason for such a situation is the lack of a systemic approach to the verification of such materials, which boils down to access to a key tool in this area, i.e. the ICSE DB, only at the national level, through the Police Headquarters in Warsaw (the Department for Combating Trafficking in Human Beings located within the structures of the Crime Bureau). Other reasons for this can be attributed to the inability to use other tools described here: a central reference database containing files in CSAM category, as well as to not having its own reliable list of *hash* values relating to material that has previously been classified as CSAM by police officers coming into contact with it in the course of their official duties. A 'reliable' list of *hash* values should be understood as a list produced as a result of a process based on a uniform CSAM classification system, taking into account the experience resulting from the exchange of information and training taking place especially at international level. The principle often applied here is that the classification given to CSAM files should be verified by three people in order to obtain full agreement in their assessment.

In addition, there are certified specialists[2] and experts[3], with specialisations in computer forensics and examination of digital data carriers, employed in the police forensic laboratories, who may also - within the framework of orders and decisions received - come into contact with content from CSAM category (Central Forensic Laboratory of the Police, 2018). Unfortunately, documents in the form of methodologies for computer and digital data carrier examination are not generally available, so issues in this area could not be included in this study. This is undoubtedly a topic for a separate publication involving representatives of this community. However, it will be useful here to refer to the scopes of activities of certified specialists and experts employed in laboratories dealing with digital data carriers and computers, published e.g. by the Forensic Laboratory of the Voivodeship Police Headquarters in Łódź. According to these, the scope of activities of a certified specialist employed in the laboratory dealing with digital data carriers includes the following:

- making image copies from visual records;
- recording of procedural acts;
- extracting frames from visual records and their editing;
- preparing demonstrative documentation;
- securing data from digital data carriers;
- making binary copies of digital data carriers;
- reading the contents of mobile phones;
- viewing, pre-selecting and converting files;
- securing records from digital video recorders.

As far as the scope of activities of an expert from the same laboratory is concerned, in addition to the

[2] The title of certified specialist entitles the holder to carry out independent technical activities, documented - in terms of their conduct and results - in a report.

[3] The title of expert, on the other hand, entitles one to independently carry out technical activities, examinations, as well as to make conclusions (art. 200 §2 item 5, Act of 6 June 1997, Code of Criminal Procedure), documented in a prepared opinion, which has a legal basis in, inter alia, art. 193 of the Code of Criminal Procedure.

above-mentioned activities, it also includes the following:

- identification of recorded objects, facilities and places based on visual records (clothing, vehicles, identification numbers/plate numbers, logos);
- identification of recording devices;
- examination of visual records to identify methods and traces of tampering with the recorded image;
- research aimed at determining facility sizes based on the recorded image;
- making other determinations possible on the basis of the analysis of visual records (e.g. selection of material, determination of the time of image recording, place of recording, equipment used for recording), (Forensic Laboratory of the Voivodeship Police Headquarters in Łódź, 2022).

In the case of the Computer Forensics Laboratory, the typical scope of activities of a certified specialist includes the following:

- securing data from computers, disks;
- making copies of data carriers;
- downloading the contents of mobile phones;
- viewing files and their pre-selection;
- file conversion.

In contrast, an expert employed in the same laboratory, in addition to the above-mentioned activities, will also:

- examine computer hardware and peripheral hardware;
- determine the purpose of computing devices, their performance and the content of their memory;
- determine and analyse the content of digital data carriers with the exception of:
  - establishing the legality, value and copyright holders of programmes, audio and video files and the content of text files,
  - determine the gender and age of the persons recorded in the files and the nature of their content (e.g.: pornography, erotica, violence, etc.),
- recover data from digital data carriers and analyse them, with the exceptions mentioned in item 3;
- examine GSM phones - read data from memory and SIM cards, (Forensic Laboratory of the Voivodeship Police Headquarters in Łódź, 2022).

It is easy to see that the activities described above are directed at two areas: the content of digital data carriers and the activity of their user, while their aim is to provide an expert's opinion on information relevant to the proceedings. In this case, the key observation for the issues analysed in this paper, concerning this group of police officers and employees, will be that their activities are therefore conducted from a completely different angle than the identification of a child and a perpetrator of a sexual offence committed against the child. According to their scopes of work, certified specialists and experts should not comment on the sex and age of the persons recorded in the files and the nature of file content, which in turn is the basis of any identification operation. On the other hand, it seems that, by virtue of their skills, these persons could lay the foundations of a new forensic specialisation dealing with the issues of victim or perpetrator identification, or cooperate with an interdisciplinary team established, for example at central level, to carry out activities in this area.

Problems affecting this professional group, which need to be resolved as a matter of priority, also include the lack of communication between laboratories, resulting in the possibility of situations where files with the same content are dealt with by unaware police officers in neighbouring units.

Restrictions of a similar nature also apply to other experts who give opinions on potentially illegal content at the request of the prosecutor's office or court. As a rule, these experts' competences are interdisciplinary and they perform their duties as experts on an ancillary basis. In addition, differences in competence between experts of different specialisations often require complementary analyses: an example of this is the cooperation of an expert sexologist and anthropologist to assess the age of a child depicted in the analysed content (comprehensive opinion). The process of assessing the content on which these experts are to comment is usually time-consuming and, in most cases, dependent on the type of audiovisual material, i.e. photos vs. videos, as well as its quantity and content. At present, a major impediment to work of these experts is the lack of standards unifying their work, especially on such key issues as the approach to the content to be assessed, i.e. each image individually vs. an overall assessment of content of a certain nature, access to training or the need for them to have visual records which may contain illegal content on their own computer equipment.

The last group of entities included in the diagram are the so-called private sector entities, comprising providers of various types of Internet products and services. It is difficult to draw the real picture of the engagement of these providers (both domestic and foreign ones), operating in Poland, in counteracting the availability of CSAM in their products and services. First of all, there is no legal requirement in Poland, as there is in the United States, for these providers to send the Dyżurnet.pl team reports on potential CSAM incidents. However, this state of affairs is likely to change significantly in the near future thanks to EU-level initiatives dedicated to this area. In July 2020, an EU strategy calling for a more effective fight against child sexual abuse was announced (European Commission, 2020), followed shortly thereafter by a new legislative proposal in the form of a Digital Services Act (European Commission, 2020) in December 2020. For the field discussed here, however, the solutions accompanying the European Commission's next legislative proposal, in May 2022, regulating the obligations of ISPs in the area of detection, reporting and removal of CSAM from their

products and services (European Commission, 2022), will be crucial. It is worth noting at this point that, almost as soon as it was announced, a global discussion began regarding the need to draw a line between measures to protect children and the privacy rights of users of these products and services.

Proposals for solutions to improve the current situation at national level

Taking into account the considerations presented in the earlier parts of this study, it should be assumed that, in the case of Poland, a significant improvement of the current situation can be achieved through the implementation of systemic solutions, within which the aforementioned entities will be able to use technological solutions available on the market. Such an approach has long been promoted by experts in the field under discussion (e.g. WeProtect, 2021).

Systemic solutions presented later in this paper at national level involve a two-pronged approach, consisting of:

- treating the the CSAM content available in cyberspace as evidence of a crime and giving it the right priority to reach child victims of real-time sexual exploitation and/or abuse first (the role of law enforcement authorities), and
- removing such content, even historical one, from cyberspace (the role of Dyżurnet.pl and the private sector).

The systemic changes advocated here, as shown in the diagram below, are therefore based on the implementation of relevant tools at national level: National CSAM Database, i.e. a database of audiovisual material depicting child sexual abuse, and lists containing *hash* values attributed to content classified as CSAM in a reliable process. A key element of these changes should be considered the enabling of communication between operating entities accessing the CSAM as part of their duties. Such functionality is offered, for example, by a solution in the form of the *Hash Check Service* (hereinafter: HCS), which has been implemented since 2019 in the Netherlands and is currently being transformed into a more advanced form, referred to as *Instant Image Identifier* (EOKM, 2022). In a nutshell, this solution allows authorised entities to send a query as to whether a file in their possession is a previously classified CSAM. This communication, using the web protocol HTTPS, takes place without the need to send the actual file - the *hash* value assigned to it is compared, via a dedicated API interface, with the contents of a set of such values managed by the Dutch organisation EOKM, already mentioned here. Depending on the results of the check, the submitter of the request receives a 'yes' or 'no' response.

The solutions proposed here include, in the first place, the Police, whose resources should include the National CSAM Database, enabling communication with field units of this formation, where materials secured in connection with proceedings conducted in Poland would be delivered. The key argument against the allegation that this would be a duplication of the ICSE database is the possibility for the Police to create their own list of *hash* values, extended each time when new content in this category is revealed and classified as part of their operations. Such activities would have a direct impact on increasing the efficiency of the service in the area discussed here. In addition, the competence to identify child victims of sexual exploitation and abuse should include specially appointed teams in police field units, carrying out operational, exploratory and investigative activities, hence the change postulated in this area is to allow access to the ICSE DB to police field units, i.e. at the level of each voivodeship, including the Warsaw Metropolitan Police.

The police list of *hash* values (only the list, not the actual files or their copies) would be made available to NASK, and in practice to the Dyżurnet.pl team, responsible for the functioning of HCS in Polish conditions. Dyżurnet.pl's task would be to manage the collected lists: its own, which would include digital signatures of files of which the Dyżurnet.pl team has been notified via dedicated channels or in cooperation with the private sector, the police list, as well as lists obtained from reliable partners such as INTERPOL, Europol, NCMEC or IWF. It is worth mentioning that similar efforts in this area have been made in the past by NASK, with the launch of the SYWENTO application. It supports the analysis of data by computer forensics experts to obtain information on whether a given Internet address (URL) contains pornographic content with a minor. A query sent to the SYWENTO application generates feedback as to whether the URLs entered into the system by the expert are present in the database of addresses identified by Dyżurnet.pl. (Dyżurnet.pl, 2022).

In addition to equipping police officers with technological tools, persons serving in teams dedicated to combating child sexual exploitation and abuse should receive mandatory, specialised training, covering the characteristics of this phenomenon, techniques for interviewing perpetrators and victims, as well as how to deal with the consequences of contact with such a specific type of crime, including the need to classify CSAM. It also seems reasonable to enrich the range of competences of police psychologists so that they can provide systemic and proactive assistance to their colleagues confronted in their work with one of the most difficult challenges of dealing with child sexual abuse material.

The possibility to submit queries to the HCS would be particularly helpful for private sector entities in Poland, which could thus verify the content of their products and services without incurring the costs associated with the individual implementation of such solutions, including the hiring and training of content moderators. In view of the changes to be brought about by the

package of EU legislative proposals in this area, such a service should be of particular interest to small and medium-sized private sector entities, for which compliance with the new regulations may constitute a significant financial burden.

The group of entities that could benefit from the functioning of the HCS would also include experts operating outside the police, for whom the possibility of making queries would contribute to increasing the efficiency of their work, as well as giving it some form of standardisation.

Summary

Cyberspace is now a place where children are groomed, solicitated and even blackmailed into obtaining sexually explicit content involving them, which translates directly into an alarming amount of such content available in this dimension. Europol representatives speak directly about the serious consequences of the increasing amount of CSAM revealed in cyberspace, year after year, for the capabilities of law enforcement agencies worldwide to identify perpetrators (Europol, 2020). In the face of such challenges, calls for the use of available technologies are therefore particularly timely.

Some efforts to change the current situation in Poland were made within the framework of a project of the Police Headquarters and the Central Forensic Laboratory of the Police called "Development of a Central Information System for Files Related to Criminal Activity", financed from 2014 to 2020 under the EU Internal Security Fund (Police, 2020), the aim of which was to develop an integrated, central system of information on files (*hashes*) related to criminal activity, called the Central Hash System. Detailed information on this subject is held by Central Forensic Laboratory of the Police, as an institution exercising substantive supervision over the project. It should be assumed that the experience gained within the framework of this project will allow for the implementation of systemic solutions postulated in this study at national level. Undoubtedly, a key element in this case will be the compatibility of the system used in this project for classifying files related to criminal activity with the system used in practice by specialists employed in Dyżurnet.pl, who are trained, among others, by INTERPOL.

Another opportunity to change the national situation was when NASK submitted a proposal for the NETTO (*Networking Enhanced Through Technological Opportunities*) project in February 2021, worth approximately

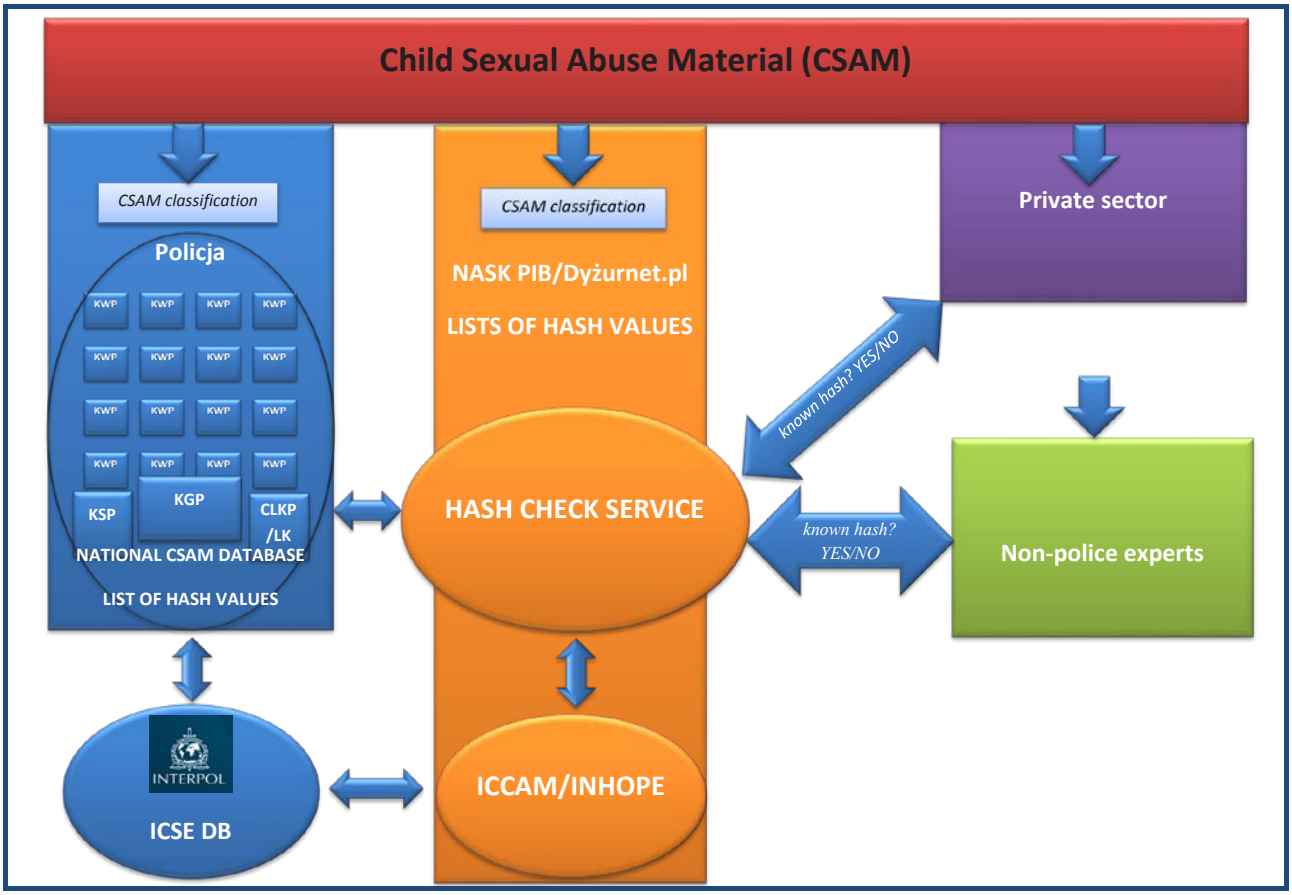


Fig. 2. Proposal to implement *hash* value exchange solutions in Poland

€1 million, under the EU's Internal Security Fund. This proposal, despite receiving a high score in the project competition, did not ultimately receive funding, which did not prejudge the re-use of the concept contained therein in another NASK project submitted to the competition a year later.

The hope for a change in the national response to the problem of child sexual exploitation and abuse can now be pinned on two recent initiatives that are significant for the area discussed here. The first one is the appointment, by Order of the Minister of Justice of 29 September 2021, of a Team for counteracting crimes against sexual freedom and morality committed to the detriment of minors (Ministry of Justice, 2021). The second initiative is the establishment of the Central Cybercrime Bureau in the Police, as of 12 January 2022 (Police, 2021). Here, it seems crucial to assume that the phenomenon of child sexual exploitation and abuse in cyberspace falls under the category of cybercrime. This assumption should be reflected in the decisions defining the organisation and competences of the newly established Bureau.

Source of figures: author

Bibliography

1. Canadian Centre for Child Protection, (2017). Survivors' survey. (Accessed on 27/01/22: https://www.protectchildren.ca/en/resources-research/survivors-survey-results/).
2. Central Forensic Laboratory of the Police, (2017). Computer forensics. (Accessed on 21/03/2022: https://clkp.policja.pl/clk/badania-i-projekty/langnodata/badania-informatyczne/153011,Badania-Informatyczne.html).
3. Central Forensic Laboratory of the Police, (2017). Decision No. 164 of the Director of Central Forensic Laboratory of the Police of 29.06.2018 on the list of forensic specialities within the scope of which opinions and reports on activities carried out in police forensic laboratories are issued.
4. Central Forensic Laboratory of the Police, (2018). Decision No. 164 of the Director of Central Forensic Laboratory of the Police of 29.06.2018 on typical scopes of work of an expert and specialist in forensic specialties.
5. Child Rescue Coalition, (2021). (Accessed on 11/10/21: https://childrescuecoalition.org/the-issue/).
6. Cybertip!ca, (2022). (Accessed on 30/05/2022: https://www.cybertip.ca/en/child-sexual-abuse/project-arachnid/).
7. Dyżurnet.pl, (2021). Report by Dyżurnet.pl 2020. (Accessed on: 11/10/21: https://dyzurnet.pl/publikacje).
8. Dyżurnet.pl, (2022). (Accessed on 30/05/2022: https://dyzurnet.pl/dla-profesjonalistow/wpis/sywento).
9. Elshenraki, H.N. (2021), Combating the Exploitation of Children in Cyberspace: Emerging Research and Opportunities. *Advances in Criminology, Criminal Justice, and Penology.*
10. EOKM, (2022). (Accessed on 30/05/2022: https://www.3-is.eu/#objectives andhttps://www.3-is.eu/sites/default/files/2022-05/iii-description-tool-v2_0.pdf).
11. Europol, (2015). (Accessed on 16/05/22: https://www.europol.europa.eu/sites/default/files/documents/efc_strategic_assessment__public_version.pdf).
12. Europol, (2017). (Accessed on 11/10/21: https://www.europol.europa.eu/newsroom/news/14-arrests-in-takedown-of-massive-child-sexual-abuse-platform andhttps://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe).
13. Europol, (2020). Internet Organised Crime Threat Assessment. (Accessed on 11/10/21: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020).
14. Europol, (2021). Internet Organised Crime Threat Assessment. (Accessed on 03/02/2022: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021).
15. Gazeta Policyjna, (2021). Numer 2 Specjalny. (Accessed on 27/01/2022: https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s).
16. INHOPE, (2020). Annual report 2020. (Accessed on 12/10/21: https://inhope.org/media/pages/the-facts/download-our-whitepapers/annual-report/bb4dd3cdc3-1628156678/inhope-annual-report-2020.pdf).
17. INHOPE, (2021). (Accessed on 11/10/21: https://www.inhope.org/EN, https://inhope.org/EN/articles/what-is-baseline).
18. INHOPE, (2022). Accessed on 21/11/22: https://inhope.org/EN/articles/the-global-standard-project.
19. Internet Watch Foundation, (2022). (Accessed on 30/05/22: https://www.iwf.org.uk/our-technology/intelligrade/ and https://www.iwf.org.uk/our-technology/crawler/).
20. INTERPOL, (2022). (Accessed on 21/11/22: https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database).
21. European Commission, (2020). 'EU strategy for a more effective fight against child sexual abuse'. (Accessed on: 03/02/2022: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agendasecurity/20200724_com-2020-607-commission-communication_en.pdf).
22. European Commission, (2020). Networks, Content and Technology, *Study on framework of best practices to tackle child sexual abuse material online: executive summary (English)*, Publications Office, 2020, https://data.europa.eu/doi/10.2759/386477.

23. European Commission, (2020). Digital Services Act. (Accessed on: 03/02/2022: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_pl).
24. European Commission, (2022). (Accessed on: 30/05/22: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472).
25. Forensic Laboratory of Voivodeship Police Headquarters in Łódź. (Accessed on: 11/07/22: https://lk-lodzka.policja.gov.pl/el8/struktura/sekcja-dokumentow/pracownia-cyfrowych-nos/606,Pracownia-Cyfrowych-Nosnikow-Danych.html and https://lk-lodzka.policja.gov.pl/el8/struktura/sekcja-dokumentow/pracownia-badan-informa/604,Pracownia-Badan-Informatycznych.html).
26. Lee, H-E., Ermakova, T., Ververis, V., Fabian, B. (2020). Detecting child abuse material: A comprehensive survey. Forensic Science International: Digital Investigation, *34*. http://doi.org/10.1016/j.fsidi.2020.301022.
27. Microsoft, (2020). (Accessed on 21/11/2022: https://blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/).
28. National Center for Missing & Exploited Children, (2020). (Accessed on 08/09/2021: https://www.missingkids.org/gethelpnow/cybertipline).
29. National Center for Missing & Exploited Children, (2020). (Accessed on 28/04/2022: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata).
30. Police, (2020). (Accessed on 08/09/2021: https://clkp.policja.pl/clk/badania-i-projekty/fundusz-bezpieczenstwa/153261,Fundusz-Bezpieczenstwa-Wewnetrznego.html).
31. Publications Office of the European Union, (2022). (Accessed on 14/06/22: https://op.europa.eu/en/publication-detail/-/publication/986ca706-cce4-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257046699 and https://op.europa.eu/en/publication-detail/-/publication/3e8e564c-cce7-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257046650).
32. Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum, 21*, 429-447. http://doi.org/10.1007/s12027-020-00625-7.
33. Council of Europe, (2021). Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse. (Accessed on 11/10/21), https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee).
34. Seto, M.C., Hanson, R.K., Babchishin, K.C. (2010). Contact Sexual Offending by Men With Online Sexual Offenses. *Sexual Abuse: A Journal of Research and Treatment*, *23*(1), 124-145. http://doi.org/10.1177/1079063210369013.
35. Act of 5 July 2018, on the National Cyber Security System (Journal of Laws 2020, item 1369, as amended).
36. Act of 6 June 1997, Penal Code (Journal of Laws 2021, item 2345, as amended).
37. Act of 6 June 1997, Code of Criminal Procedure (Journal of Laws 2021, item 534 as amended).
38. Act of 17 December 2021, amending certain acts in connection with the establishment of the Central Cybercrime Bureau (Journal of Laws 2021, item 2447).
39. Wasilewski, J. (2013). Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego*, *9*, 225-234.
40. WeProtect, (2021). The Model National Response. (Accessed on 03/02/2022: https://www.weprotect.org/model-national-response/).
41. Web-IQ, (2020). EU Strategy proposal CSAM lifecycle and interception. (Accessed on 08/09/2021: https://vimeo.com/434684287).
42. Order of the Minister of Justice of 29 September 2021 on the appointment of a Team for counteracting crimes against sexual freedom and morality to the detriment of minors. (Accessed on 03/02/2022: https://www.gov.pl/web/sprawiedliwosc/du-21-233).

Translation GTC AMG sp. z o.o.