 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).

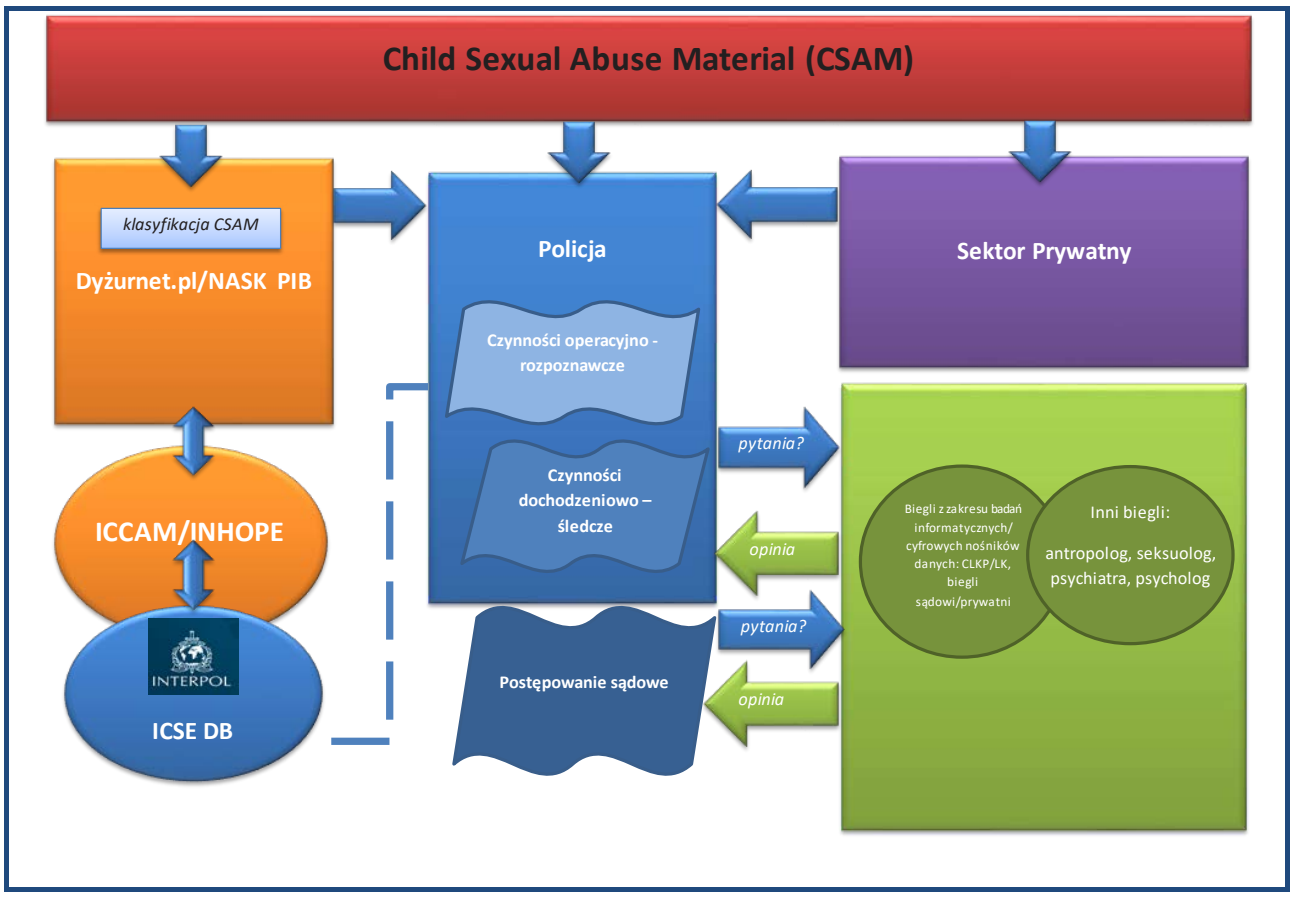
Aktualna sytuacja w Polsce

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).

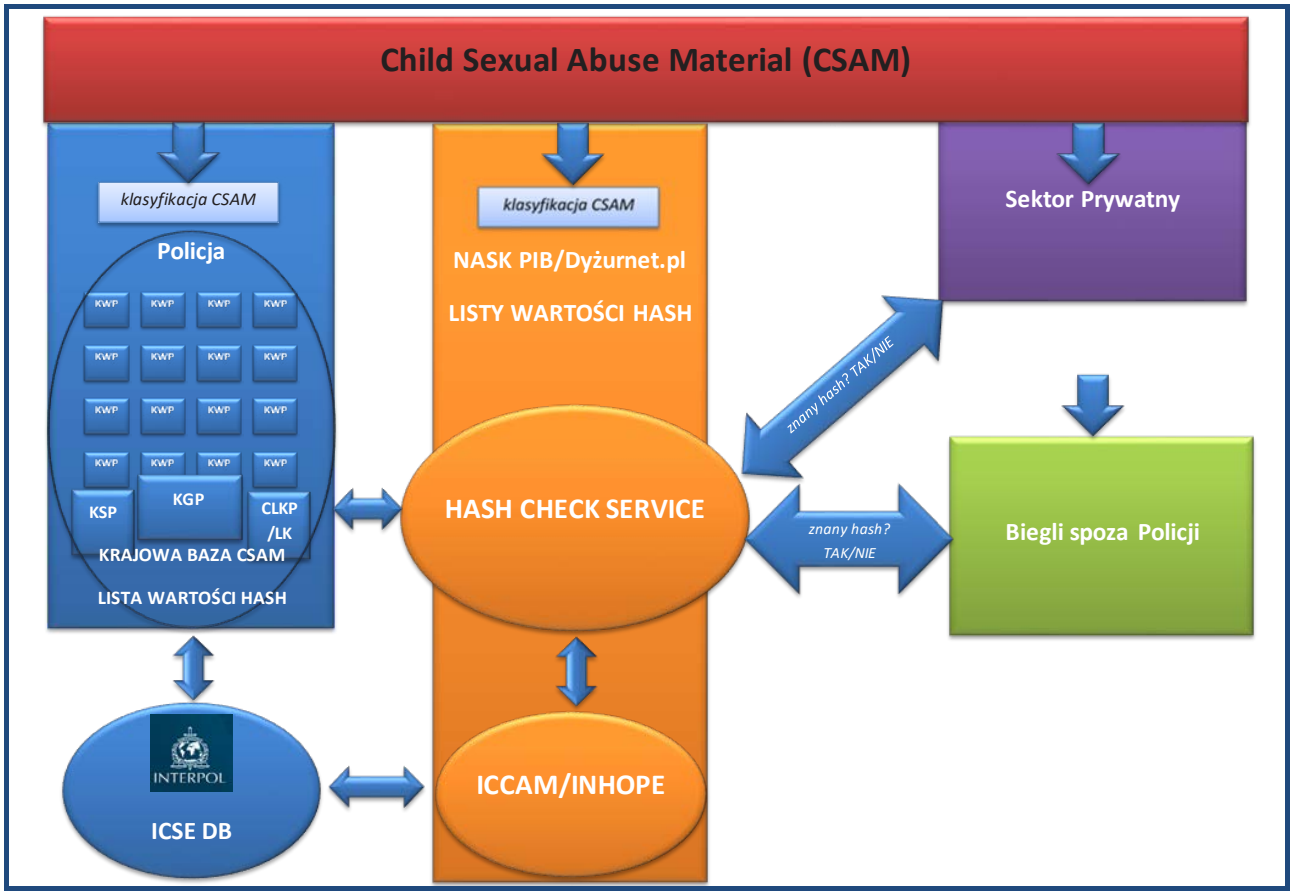
Postulowane tu zmiany systemowe, przedstawione na zamieszczonym poniżej schemacie, opierają się zatem na wdrożeniu stosownych narzędzi na poziomie krajowym: Krajowej Bazy CSAM, tj. bazy materiałów audiowizualnych przedstawiających wykorzystywanie seksualne dzieci, oraz list zawierających wartości *hash* 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).