Zwalczanie seksualnego wykorzystywania dzieci w internecie na przykładzie CSAEM i OCSAE. Wyzwania technologiczne i metodologiczne

Paweł Oberszt

NASK PIB, Dział Reagowania Na Nielegalne Treści w Internecie Dyżurnet.pl

Ochrona dzieci przed zorganizowaną, transgraniczną cyberprzestępczością jest zagadnieniem złożonym. Wymaga nieustannej walidacji działań m.in. w obszarze edukacji, prawa, technologii, współpracy międzyinstytucjonalnej i międzysektorowej, a także udoskonalania aparatu pojęciowego, którym opisujemy powiązane z nią zjawiska. Artykuł koncentruje się na wybranych wyzwaniach technologicznych, podczas omawiania których poruszanych jest kilka zagadnień metodologicznych związanych ze zwalczaniem seksualnego wykorzystywania dzieci, ze szczególnym uwzględnieniem CSAEM (ang. Child Sexual Abuse and Exploitation Materials*) oraz OCSAE (ang.* Online Child Sexual Abuse and Exploitation Materials*).*

CSAEM mogą stanowić świadectwo prawdziwych, traumatyzujących zdarzeń lub być zmodyfikowane i/lub wygenerowane w pełni cyfrowo. OCSAE to forma cyberprzestępczości wymierzonej w małoletnich, której skuteczne zwalczanie wymaga z jednej strony adekwatnej taksonomii sprawców, z drugiej zaś – stosowania coraz to lepszych rozwiązań umożliwiających skuteczne wykrywanie i zabezpieczanie w sieci dowodów tego typu czynów zabronionych.

Nowoczesne narzędzia informatyczne – takie jak specjalistyczne, dedykowane programy komputerowe, bazy CSAM (ang. Child Sexual Abuse Materials*), które zawierają m.in. pliki z wizerunkami pokrzywdzonych, ich klasyfikację oraz hasze, platformy wymiany informacji,* crawlery *i* scrapery *czy rozwiązania oparte na AI – pozwalają przetwarzać dane cyfrowe rzędu wielkości terabajtów, a nawet petabajtów, w sposób precyzyjny i co najmniej (semi)zautomatyzowany. Uzyskane wyniki (również te o charakterze predykcji, np. w zakresie kategoryzacji treści, identyfikacji pokrzywdzonych czy*

 https://doi.org/10.63237/QGKJ1491

geolokalizacji) przyśpieszają uzyskanie dowodów istotnych z punktu widzenia wykonywanych czynności, skracają czas ekspozycji na treści CSAEM, a przede wszystkim ułatwiają dotarcie do nieznanych materiałów przedstawiających seksualne wykorzystywanie osób małoletnich, które z kolei mogą prowadzić do samych dzieci.

Myślą przewodnią artykułu jest założenie, że wdrożenie analogicznych funkcjonalnie rozwiązań w Polsce wzmocni krajową i międzynarodową współpracę organów ścigania i wymiaru sprawiedliwości z siecią hotline'ów INHOPE, w tym z polskim Dyżurnet.pl NASK PIB, a także z ICP (ang. Internet Content Provider*) czy ISP (ang.* Internet Service Provider*), przyczyniając się do skuteczniejszej ochrony najmłodszych użytkowników cyberprzestrzeni.*

Słowa kluczowe:
CSAM; CSAEM; OCSAE; małoletni; cyberprzestępczość zorganizowana; technologie

Wstęp

Seksualne wykorzystywanie i eksploatacja, których ofiarami stają się małoletni (CSAE), istnieją co najmniej od czasów starożytnych (Nijakowski, 2010, s. 309–353; Rosli i in., 2018; Krać-Batyra i in., 2025). Z uwagi na ograniczony charakter artykułu i akcentowanie innych obszarów badawczych zróżnicowany i powszechny charakter tego zjawiska zostanie zarysowany za pomocą trzech – za to bardzo wyrazistych w przekazie – cytatów. Dają one wyobrażenie tego, jak na przestrzeni wieków ujmowano pozycję dziecka w społeczeństwie (również tym cyfrowym), jego prawo do podmiotowości i ochrony:

> W naszej oświeconej epoce nie otaczają nas niewolne kwiatuszki, które można by zrywać sobie od niechcenia między transakcją a łaźnią, jak to robiono w epoce rzymskiej; i nie czynimy tak, jak w jeszcze bardziej luksusowych czasach czynili dystyngowani ludzie Wschodu, gdy między baraniną a sorbetem z róży zażywali (…) maleńkich pocieszek. W tym cały szkopuł, że ogniwo, które dawniej spajało dorosły świat z dziecięcym, całkowicie przecięły nowe obyczaje i prawa (Nabokov, 2024, s. 162).

> Przemoc seksualna wobec dzieci oraz ich wykorzystywanie były niegdyś ograniczone do fizycznych miejsc, takich jak szkolne place zabaw, przedsionki kościołów, domy zaufanych sąsiadów, wycieczki szkolne oraz obskurne, słabo oświetlone zaplecza księgarni dla dorosłych. Gwałtowny wzrost liczby użytkowników internetu stworzył

> sprawcom polującym na dzieci przestrzeń do wirtualnych łowów i napędził dynamiczny, wielomiliardowy handel powiązanymi z nielegalnymi materiałami[1] (Ferraro i in., 2005, s. 3).
>
> Dzieci są konsumentami w cyfrowych ekosystemach, często projektowanych tak, aby maksymalizować zaangażowanie i zysk. Platformy, napędzane przez mało transparentne systemy sztucznej inteligencji, przyczyniają się do kształtowania percepcji, zachowań i światopoglądu dzieci – nie zawsze w ich najlepszym interesie (UNICEF Innocenti, 2025).

Cyberprzestępczość seksualna na szkodę dzieci (OCSAE) może być traktowana jako przeniesiona do internetu, ale nadal raczej geograficznie ograniczona (a wręcz lokalna), forma znanych od dawna czynów zabronionych popełnianych przez dewiantów seksualnych, którzy mają wystarczającą wiedzę techniczną, żeby stosować unowocześnione *modus operandi* (Sajkowska, 2003; Aiken i in., 2011; Bocheński, 2015; Steel i in., 2021; Kavruk i in., 2026). Może być również postrzegana jako zdywersyfikowana w metodach i środkach, motywowana m.in. finansowo, zorganizowana przestępczość transgraniczna (KE, 2007[2]; Bielawski, 2020; Kierznowski, 2025; Europol, IOCTA 2011–2025), wykorzystująca nie tylko najnowsze osiągnięcia technologiczne (Bursztein i in., 2019; ICMEC i in., 2021, WeProtect, 2025a) czy nowe metody popełniania przestępstw (Europol, 2025a; IWF, 2023; Dyżurnet.pl, 2026), ale także adaptująca coraz to skuteczniejsze formy kontrwykrywczej (ang. *anti-forensics*) aktywności (Van de Sandt, 2019; Majed i in., 2020; Chlebowicz i in., 2022).

W niniejszym artykule poświęconym ochronie dzieci w cyberprzestrzeni skupiono się na tej drugiej postaci (zaliczanej niekiedy do tzw. zorganizowanej przestępczości hedonistycznej), a także technologiach i metodach, które mogą pomóc w jej zwalczaniu. Taką perspektywę przyjął m.in. Europol, który już kilkanaście lat temu umiejscawiał OCSAE w kontekstach właściwych zorganizowanym grupom przestępczym:

1 Tłumaczenia źródeł obcojęzycznych pochodzą od Autora.

2 Komisja Wspólnot Europejskich blisko 20 lat temu opublikowała *Komunikat do Parlamentu Europejskiego, Rady oraz Komitetu Regionów – W kierunku ogólnej strategii zwalczania cyberprzestępczości* (2007). Poczyniła tam następujące obserwacje (pkt 1.2.1): „Trudno jest uzyskać dokładny obraz obecnej sytuacji ze względu na ciągły rozwój przestępczości i brak wiarygodnych informacji. Można jednak zauważyć kilka ogólnych trendów: a) liczba przestępstw informatycznych stale wzrasta, działania przestępcze stają się też coraz bardziej wyrafinowane i wykraczają poza granice państwowe; b) wyraźne przesłanki wskazują na rosnący udział w cyberprzestępczości zorganizowanych grup przestępczych; c) nie wzrasta jednak liczba aktów oskarżenia na podstawie transgranicznej współpracy oddziałów ścigania w Europie".

> Chociaż powszechnie przyjmuje się, że sprawcy wykorzystywania seksualnego dzieci (…) nie tworzą typowych zorganizowanych grup przestępczych, to na takich platformach organizują się oni w analogiczną strukturę hierarchiczną. Ma to zazwyczaj miejsce na platformach, na których sprawcy wymieniają materiały przedstawiające seksualne wykorzystywanie dzieci (…). W tym środowisku osoby dostarczające materiały uznawane za „wysokiej jakości" (zazwyczaj nowe, wcześniej nieznane treści), wykazujące się wysokim poziomem wiedzy technicznej oraz dzielące się dobrymi praktykami, mogą osiągać najwyższy status w grupie (ang. *achive highiest ranks*) i zyskiwać rozpoznawalność w swoich kręgach. Ponadto niektórzy sprawcy nawiązują współpracę między sobą w celu dzielenia się fizycznym dostępem do dzieci (ang. *to share physical access to children*), co ułatwia produkcję nowych materiałów oraz ich personalizację (IOCTA, 2014, s. 29).

Rozwijająca się od lat cyberprzestępczość wymusza na organach ścigania i wymiarze sprawiedliwości szukania coraz to nowszych sposobów jej przeciwdziałania. Znane od dawna taksonomie sprawców czy rozwiązania teleinformatyczne – co zostanie wykazane w niniejszym artykule – muszą podlegać ciągłej ocenie adekwatności i skuteczności. Jedynie bowiem ich adaptacja do zmiennych warunków cyberprzestrzeni umożliwi detekcję, zabezpieczanie i dowodowe wykorzystanie (np. w procesie karnym) informacji i danych związanych z CSAEM (również tych wytwarzanych np. przy użyciu sztucznej inteligencji). Dotyczy to m.in. omawianych tu technologii, które powinny być wdrażane i rozwijane zarówno po stronie ICP/ISP, jak i podmiotów zaangażowanych w zwalczanie CSAEM i OCSAE (np. *hotline'y*, instytucje naukowo-badawcze, organy ścigania i wymiaru sprawiedliwości).

Poniższa, mająca już tylko historyczne znaczenie grafika (rys. 1) stanowi doskonałe świadectwo zmienności OCSAE. Dokumentuje ona – w perspektywie dwudziestoletniej – dynamikę korzystania z kanałów dystrybucji materiałów przedstawiających seksualne wykorzystywanie dzieci (Bursztein i in., 2019, s. 2605). Na przykładzie chociażby: wiadomości e-mail (tu: Email), stron internetowych (tu: URL) oraz komunikatorów (tu: Instant Messanger), doskonale widać, że zmiany metod i narzędzi organów ścigania powinny następować wraz ze zmianą *modus operandi* sprawców. Inaczej bowiem analizuje się sieci P2P, inaczej – komunikatory (obecnie w dużym stopniu zabezpieczone szyfrowaniem typu end-to-end, tj. E2EE), a zupełnie inaczej (nieujętą jeszcze w tej grafice) jedną z najtrudniejszych do zabezpieczenia form OCSAE, tj. *live streaming*. Truizmem jest stwierdzenie, że kanały pozostające poza monitoringiem oznaczają niekontrolowane rozprzestrzenianie się treści CSAEM i zwielokrotniają wiktymizację.

Rys. 1.

Dystrybucja CSAEM według kryterium technologii rozpowszechniania (1998–2017) (Bursztein, i in., 2019, s. 2605)

	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
FTP	9%	10%	22%	25%	9%	5%	3%	6%	1%	1%	1%	1%	0	1%	1%	0	1%	0	2%	0
Email	0	1%	1%	2%	9%	16%	18%	8%	3%	4%	6%	4%	3%	4%	3%	4%	5%	4%	3%	2%
P2P	0	0	0	2%	9%	10%	7%	9%	11%	11%	6%	6%	5%	2%	1%	1%	2%	7%	1%	9%
Chatroom/ IRC	1%	1%	1%	1%	2%	2%	3%	3%	7%	10%	6%	3%	2%	1%	2%	2%	2%	5%	22%	23%
Instant Messanger	1%	1%	1%	2%	3%	3%	3%	3%	10%	17%	7%	4%	2%	2%	4%	2%	3%	1%	13%	19%
Forum	2#	4%	3%	3%	4%	2%	4%	5%	5%	7%	3%	6%	7%	24%	2%	2%	2%	2%	7%	4%
Gaming	0	0	0	0	0	0	0	0	0	12%	18%	5%	3%	3%	7%	8%	9%	9%	15%	10%
SMS	0	0	0	0	0	0	0	0	0	1%	13%	12%	10%	18%	12%	13%	8%	4%	7%	1%
Cell phone	0	0	0	0	0	0	0	0	0	0	0	2%	2%	1%	4%	10%	11%	17%	27%	25%
Tor	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2%	3%	5%	26%	42%	22%
URL	0	0	0	0	0	0	0	0	0	0	0	0	1%	1%	2%	2%	5%	10%	39%	26%

Z uwagi na fakt, że artykuł ma charakter przeglądowy, temat technologii dystrybucji, a także badań nad nimi zostanie rozwinięty w kolejnej publikacji, uwzględniającej m.in. analizy INHOPE, IWF oraz Dyżurnet.pl, a także systemowe podejście na poziomie krajowym i instytucjonalnym (na przykładzie wybranych państw, w tym Polski). W niniejszym tekście zostaną natomiast prześledzone dedykowane, skalowalne narzędzia dostępne organom ścigania i wymiarowi sprawiedliwości.

Język – narzędzie do walki z CSAEM i OCSAE

Precyzyjny i dostosowany do płynnej rzeczywistości aparat pojęciowy – czy to w odniesieniu do ustalania znamion kodeksowych, czy siatki terminologicznej wykorzystywanej w badaniach, czy wreszcie jako relewantny element procesu klasyfikacji CSAEM[3] (i zjawisk towarzyszących) – stanowi jedno z narzędzi pozwalających reagować na tę odmianę cyberprzestępczości.

Autor podziela pogląd, że język to element walki z seksualnym wykorzystywaniem dzieci (Adler, 2001; Dąbrowska, 2025; ECPAT, 2025a), ale zwraca również uwagę na fakt, że może być tego wykorzystywania kolejnym elementem:

> Reasumując, pierwszy poziom wiktymizacji może być następstwem przestępstwa kontaktowego, które miało miejsce w świecie fizycznym. Drugi poziom odnosi się do szeroko pojętej cyberprzestrzeni oraz technologii związanych z utrwalaniem, przetwarzaniem czy też wytwarzaniem rzeczywistości w postaci zapisów audio-wizualnych. Trzeci zaś poziom wiktymizacji odnosi się do języka opisującego dwa wcześniejsze. (…) to perwersyjny język dyskursu (np. medialnego, prawnego, naukowego) opisującego przestępstwa seksualne na szkodę dzieci (Krać-Batyra i in., 2025, s. 26).

Zacznijmy zatem od objaśnienia podstawowych pojęć, których zapamiętanie i uporządkowanie powinna ułatwić poniższa wizualizacja (rys. 2). W dyskursie międzynarodowym stosuje się szereg akronimów i definicji odnoszących się do treści oraz czynności seksualnych naruszających dobro małoletnich. Utrwalenie, zwłaszcza

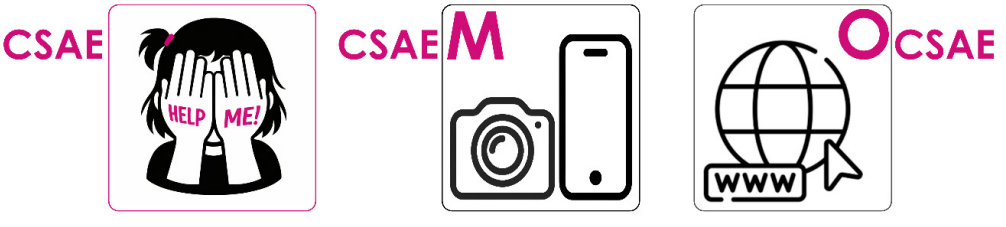
3 Autor stosuje akronim CSAEM (ang. *Child Sexual Abuse & Exploitation Materials*) jako zbiorczą nazwę dla treści związanych z seksualnym krzywdzeniem dzieci (zarówno wykorzystywaniem, jak i eksploatacją). W tłumaczeniu akronimu CSAEM na język polski stosowany jest natomiast uproszczony zapis: „materiały przedstawiające seksualne wykorzystywanie dzieci". W odniesieniu do baz zawierających hasze, klasyfikację i materiały audiowizualne konsekwentnie używa się w artykule akronimu CSAM.

w postaci audiowizualnej, aktywności przestępczej w postaci seksualnego wykorzystywania i eksploatacji dzieci (ang. *Child Sexual Abuse & Exploitation*, CSAE) ewoluuje wraz z technologiami pozwalającymi na rejestrowanie, multiplikację, a także wytwarzanie materiałów (równolegle stosuje się określenia: treści, zapisy, obrazy).

Zwykle przyjmuje się, że materiały przedstawiające seksualne wykorzystywanie i eksploatację dzieci (CSAEM) przybierają postać plików (np. zdjęć i wideo) czy transmisji na żywo (ang. *live streaming*). W makroperspektywie należy jednak mówić o forach i subforach, stronach internetowych, a co za tym idzie – o rozwiązaniach chmurowych i przestępczej infrastrukturze, opartej na łatwych do multiplikacji i przeniesienia serwerach.

W odniesieniu do cyberprzestrzeni Autor preferuje występujące powszechnie w literaturze anglojęzycznej (Ali i in., 2021; Caffo, 2021; Brown, 2023) określenie OCSAE (ang. *Online Child Sexual Abuse and Exploitation*), które odnosi się do szerokiej kategorii zachowań przestępczych w sieci. Obejmuje ono różnorodne formy przemocy seksualnej wobec dzieci. Wspólnym i dominującym elementem, ułatwiającym przedmiotowe wykorzystanie, są technologie teleinformatyczne. Do tej grupy zalicza się m.in. uwodzenie małoletnich (ang. *grooming*), nakłanianie dzieci do wytwarzania CSAEM w środowisku online, np. podczas wspomnianej już transmisji wideo (ang. *live-streaming of child sexual abuse*), rozpowszechnianie i monetyzację takich treści (ICMEC, 2021; Celiksoy i in., 2023; Childlight, 2025; INHOPE, 2025a), szantaż na tle seksualnym (ang. *sextortion*), a także generowanie materiałów CSAEM z wykorzystaniem narzędzi sztucznej inteligencji (ang. *Artificially Generated* CSAEM, AIG CSAEM), w tym na podstawie neutralnych fotografii pozyskiwanych z mediów społecznościowych, stron placówek szkolnych, czy w związku z tzw. *sharentingiem* (Bongen i in. 2021; Dyżurnet.pl, 2021).

Rys. 2.
Podstawowe terminy: CSAE, CSAEM, OCSAE (opracowanie: Dyżurnet.pl)



Typologia sprawców związanych z cyberprzestępczością seksualną na szkodę dzieci

Zagadnienia związane z aparatem pojęciowym służącym do opisu CSAEM i OCSAE ściśle wiążą się z taksonomią sprawców. Autor proponuje przyjąć, że istnieje korelacja między skutecznością ich wykrywania i zwalczania a adekwatnym określeniem *modus operandi*.

Stereotypowe myślenie o sprawcach przemocy seksualnej na szkodę dzieci (np. dewiant, mężczyzna, osoba z przeciętnymi umiejętnościami z zakresu IT) może prowadzić do zaniechania czynności operacyjno-rozpoznawczych czy też procesowych, w tym działań transgranicznych wymierzonych w zwalczanie motywowanej finansowo cyberprzestępczości zorganizowanej. Prawidłowe rozpoznanie charakteru przestępczości i wstępne profilowanie sprawcy to podstawa do dalszego „sukcesu" procesu karnego, a więc skutecznego przeciwstawienia się przestępczości z XXV rozdziału Kodeksu karnego, w tym ochrony osób małoletnich.

W 2014 r. cykliczny raport *Internet Organised Crime Threat Assessment*, tj. IOCTA (Europol, 2014a, s. 10), podaje, że sprawcy związani z CSAEM i OCSAE: „korzystają z wielu tych samych usług i narzędzi co typowi cyberprzestępcy, w tym z narzędzi anonimizujących, bezpiecznej poczty elektronicznej, hostingu typu *bulletproof* oraz walut wirtualnych". Z podobnego założenia wychodzili autorzy, którzy zaczęli dostrzegać różnorodność sprawców przestępstw seksualnych na szkodę dzieci, i tę wiedzę operacjonalizować – np. w postaci typologii użytkowników CSAEM.

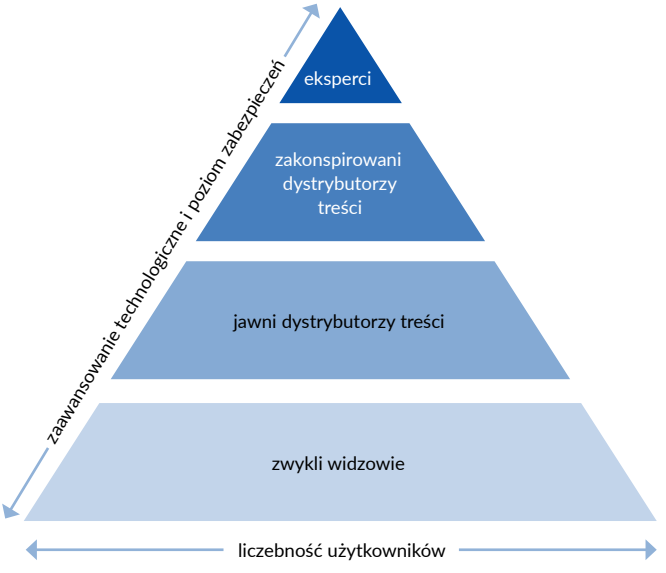
Początkowo skupiano się na rozróżnieniu dwóch przeciwstawianych sobie typów aktywności przestępczej. Jednakże, na co zwraca uwagę m.in. Durkin, był to podział niewystarczający:

> Chociaż sprawcy przestępstw seksualnych w internecie byli tradycyjnie przedstawiani na skali dychotomicznej jako „podróżnicy" i „handlarze", ich zachowania nie zawsze wzajemnie się wykluczały. Mogły być częścią kontinuum zachowań: sprawca zaczynał od oglądania, pozyskiwania, wytwarzania i udostępniania pornografii dziecięcej, by później przejść do działań takich jak czatowanie, *grooming* i ostatecznie spotkanie z małoletnim w celach seksualnych (Durkin i in., 2012, s. 803).

Do chwili obecnej spotyka się zwizualizowane poniżej (rys. 3) stosowanie „typologii sprawców treści internetowych (Moran, 2010), skoncentrowanej na gromadzeniu CSAEM i opartej na doświadczeniach zdobytych podczas monitorowania i ścigania internetowych sprawców przestępstw seksualnych w tym obszarze. Kategorie przedstawiają się następująco: zwykli widzowie (ang. *simple viewers*) – początkujący,

którzy mogą być jedynie ciekawi CSAEM; jawni dystrybutorzy treści (ang. *open traders*) – sprawcy rozpowszechniający CSAEM online; zakonspirowani dystrybutorzy treści (ang. *closed traders*) – dystrybutorzy nielegalnych treści o wysokim poziomie zabezpieczeń, funkcjonujący w społecznościach o ograniczonym z zewnątrz dostępie; oraz eksperci (ang. *experts*) – wieloletni, zaangażowani sprawcy, dla których kwestie bezpieczeństwa stanowią istotny element działania. Trójkątny kształt przedstawia hipotetyczny model rozkładu sprawców" (Aiken i in., 2011, s. 6–7).

Rys. 3.
Typologia Morana z typami użytkowników CSAEM (Aiken i in., 2011, s. 22)



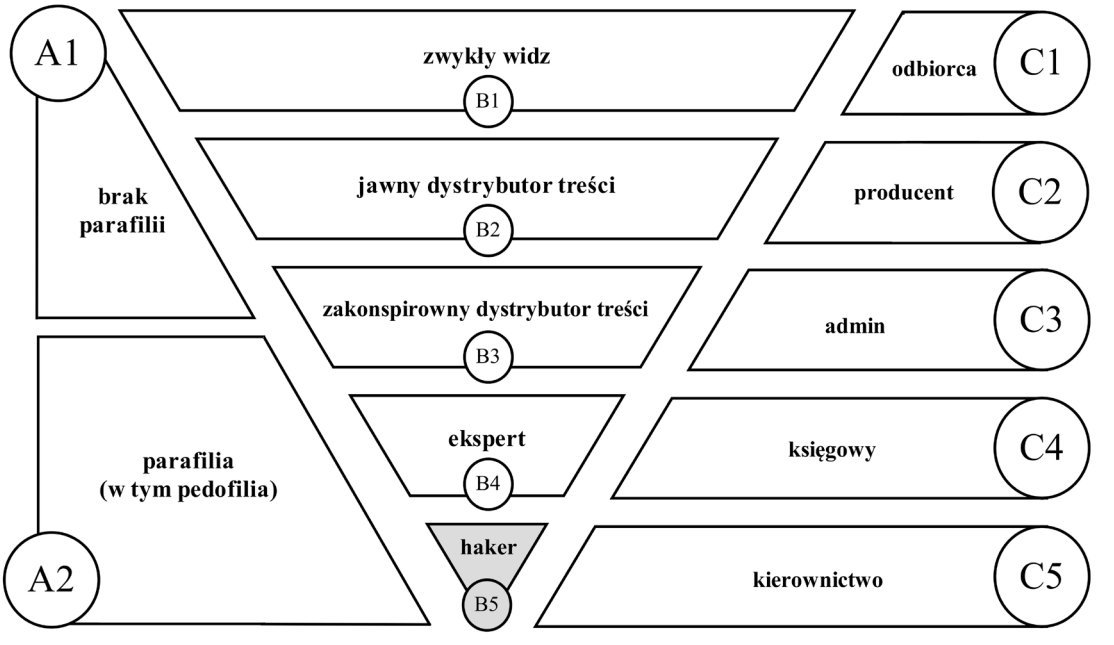
Biorąc pod uwagę cytowaną w niniejszym tekście literaturę, badania i raporty, Autor proponuje zaktualizowany (obszary wyróżnione kolorem szarym) i rozszerzony model (rys. 4). W pierwszej kolejności należy bardzo uważnie przyjrzeć się seksualności sprawców pod kątem potwierdzenia bądź wykluczenia parafilii (Bocheński, 2015).

W poniższej grafice odpowiada za to lewa część matrycy z dwoma zmiennymi: A1 – brak parafilii, A2 – stwierdzona parafilia (w tym pedofilia). W części środkowej uwzględniono (również wizualnie) typologię Morana (zmienne: B1÷B4). Dodano jednak kolejny typ użytkownika, ujęty jako zmienna B5 – haker. Organy ścigania obserwują ten typ sprawcy, tj. użytkownika CSAEM, który traktuje go jak narzędzie ataku (analogicznie do *malware*), przedmiot finansowego szantażu (analogicznie do *ransomware*) czy rodzaj środka do kompromitacji (analogicznie do *data breach*/*data leak*).

Nowością – w stosunku do klasyfikacji Morana i podziału na sprawców ze względu na stwierdzoną parafilię – jest dodanie poziomu zorganizowania wyrażonego w części prawej matrycy. Poszczególnym zmiennym (C1÷C5) przypisano wstępnie zdefiniowane role organizacyjne, które w kompleksowym budowaniu profilu sprawcy należy równolegle oceniać i badać ze zmiennymi z grup A i B.

W odniesieniu do zmiennych C1–C2 oraz C5 powinny być one zrozumiałe same przez siebie. W zmiennej C3 uwzględniono osoby posiadające wysokie zdolności techniczne i wykorzystujące je do świadczenia usługi w modelu CaaS (ang. *Crime as a Service*), np. poprzez wspomniany już BPH (ang. *bulletproof hosting*), czyli odporną infrastrukturę umożliwiającą bezpieczne działanie przestępców związanych z seksualnym wykorzystywaniem dzieci (Alrwais i in. 2017, s. 807; Europol, 2020, s. 20; DeutscheWelle, 2021). Zmienną C4 przydzielono osobom odpowiadającym za przepływy i rozliczenia finansowe (The Financial Crime News, 2021, s. 76, 86).

Rys. 4.
Matryca ABC – typologia sprawców przestępstw seksualnych (opracowanie własne)



Przedstawiona tu propozycja matrycy zawierającej typologię sprawców związanych z cyberprzestępczością seksualną na szkodę dzieci zwraca uwagę na kompleksowe do nich podejście zarówno od strony opiniowania przez biegłych – np. z zakresu seksuologii (A1–A2), specjalistów z dziedziny informatyki śledczej zorientowanej na obraz (B1–B5) – jak i analityków zajmujących się przestępczością zorganizowaną (C1–C5). Zagadnienie to wymaga dalszych pogłębionych studiów (np. w postaci badań aktowych w kraju oraz – z uwagi na transgraniczny charakter CSAEM i OCSAE – za granicą).

Przywołana poniżej statystyka typów zjawisk raportowanych w NCMEC – największej amerykańskiej organizacji zajmującej się ochroną dzieci o zasięgu międzynarodowym (raporty NCMEC dotyczą również Polski, a ich odbiorcami są krajowe organy ścigania) – wskazuje na potrzebę rewizji powszechnego poglądu, że każda osoba popełniająca przestępstwo seksualne na szkodę osób małoletnich to (jedynie) pedofil w rozumieniu osoby ze stwierdzoną parafilią jako jednostką chorobową (ICD-11 czy DSM-5). Świadomość zmian w działaniu sprawców z kolei powinna wymuszać na organach ścigania i wymiarze sprawiedliwości nowe metody prac (porównaj przedstawione powyżej etapy rozwoju informatyki śledczej) i korzystanie z coraz to bardziej zaawansowanych narzędzi, które umożliwią m.in.:

- co najmniej (semi)automatyczną klasyfikację i kategoryzację dużych woluminów treści opartą o wiarygodne (zgodne z krajowym systemem prawnym) wartości hasz, referencyjną bazę materiałów CSAEM czy predykcje uzyskiwane dzięki sztucznej inteligencji;
- analizę portfeli kryptowalutowych (i innych narzędzi płatniczych) służących do ukrywania operacji finansowych związanych z seksualnym wykorzystywaniem dzieci;
- wyszukiwanie powiązań i relacji osób, urządzeń, miejsc czy obrazów;
- wykorzystanie rozszerzonego zestawu standardowych słów kluczowych, służących do wyszukiwania treści CSAEM (np. '1yo', 'teen', 'lolita') o nazwy narzędzi płatniczych, czy żargon związany z formami przemocy, manipulacji lub ekstremistycznych praktyk religijnych[4].

Warto odnotować, że nie istnieją narzędzia typu *all-in-one*, czyli zawierające wszystkie istotne funkcje. Bardzo często wymagane i znacznie efektywniejsze jest korzystanie z kilku, dedykowanych do danego obszaru rozwiązań. Omówione w dalszej części technologie o zasięgu międzynarodowym stanowią egzemplifikację ww. funkcji.

4 Por. np. https://www.dfir.training/downloads/search-terms?category[0]=6&category_children=1

Perspektywa międzynarodowa zwalczania CSAEM i OCSAE

Organizacje takie jak Interpol (Interpol, 2022a, 2025), Europol (Europol, 2025b, 2025c), Argos (ForensicsFocus, 2018), INHOPE (INHOPE, 2024; Universal Classification Schema, 2025b), National Center for Missing & Exploited Children (NCMEC, 2025; Tech Coalition, 2022), Internet Watch Foundation (IWF, 2021, 2025) czy Canadian Centre for Child Protection (C3P), albo kraje jak Francja (Billuart i in., 2025) czy Wielka Brytania (HMICFRS, 2023) od dawna – w celu kompleksowej ochrony dzieci – opracowują, wdrażają, a ponadto upowszechniają nowe rozwiązania legislacyjne, technologiczne czy formy kooperacji krajowej i międzynarodowej.

Statystyki INHOPE, Europolu, krajowego Dyżurnet.pl (Dział Reagowania na Nielegalne Treści w Internecie, stanowiący część CSIRT NASK PIB) czy NCMEC mówią o wciąż rosnącej liczbie treści CSAEM i sprawców lub też grup specjalizujących się w OCSAE. Przedstawiona poniżej tabela zestawia liczbę raportów NCMEC z 2024 r. i 2025 r. (tabela 1) dotyczących pięciu różnych zjawisk. W trzech pierwszych nastąpił wzrost około dwukrotny, natomiast ostatnie dwie zanotowały odpowiednio około dwunasto- i sześćdziesięciokrotny wzrost.

Tabela 1.

Dynamika wybranych zjawisk na podstawie raportów NCMEC z lat 2024–2025 (opracowanie własne na podstawie: Davis, 2025)

	2024 (I połowa)	2025 (I połowa)
Uwodzenie (dziecka) **w internecie** (ang. *online enticement*)	292 951	518 720
Uwodzenie (dziecka) **w internecie motywowane sadyzmem** (ang. *sadistic online enticement*)	508	1093
Szantaż na tle seksualnym motywowany finansowo (ang. *financial sextortion*)	13 842	23 593
Handel dziećmi w celu ich seksualnego wykorzystywania (ang. *child sex trafficking*)	5976	62 891
Treści wytworzone/przetworzone z użyciem sztucznej inteligencji (ang. *generative Artificial Intelligence*)	6835	440 419

Powyższe zestawienie określa dynamikę przestępstw powiązanych z CSAE, a także wskazuje charakter najnowszych zjawisk. I tak przykładowo obok handlu dziećmi w celu ich seksualnego wykorzystywania (domyślnie można tu założyć motywację seksualną po stronie „nabywcy" oraz finansową – „sprzedawcy") występują także aktywności przestępcze motywowane sadyzmem lub korzyściami finansowymi.

W odniesieniu do specjalizujących się grup sprawców warto nadmienić o kontrdziałaniach, realizowanych np. w Wielkiej Brytanii (Hydrant Programm, 2024).

Wśród badań i inicjatyw podejmowanych przez międzynarodowe instytucje zajmujące się szeroko pojętą ochroną dzieci przed OCSAE – na przykładzie takich podmiotów jak TechCoallition (TechCoalition, 2025b, 2025c), Thorn (Thorn, 2024a, 2025), Stanford Internet Observatory (Grossman, 2024) czy OECD (OECD, 2023, 2025) – wyróżnić można dwa zasadnicze kierunki działań powiązanych z tematem artykułu. Po pierwsze, bada się samą technologię w jej dwóch aspektach, tj. umożliwiającą seksualne wykorzystywanie dzieci online oraz służącą do przeciwdziałania temu zjawisku. Po drugie, dokonuje się wszechstronnych analiz platform (lub szerzej: dostawców usług), w przestrzeni których występują te zjawiska.

W tym drugim kontekście warto wspomnieć tzw. teorię przestrzeni bezprawia (ang. *lawless space theory*), która podkreśla, że anonimowy i niechroniony przez państwo czy podmioty prawa międzynarodowego internet to miejsce idealne do popełniania dowolnego rodzaju przestępstw, w tym CSAEM i OCSAE (Steel i in., 2022; Europol, 2025d).

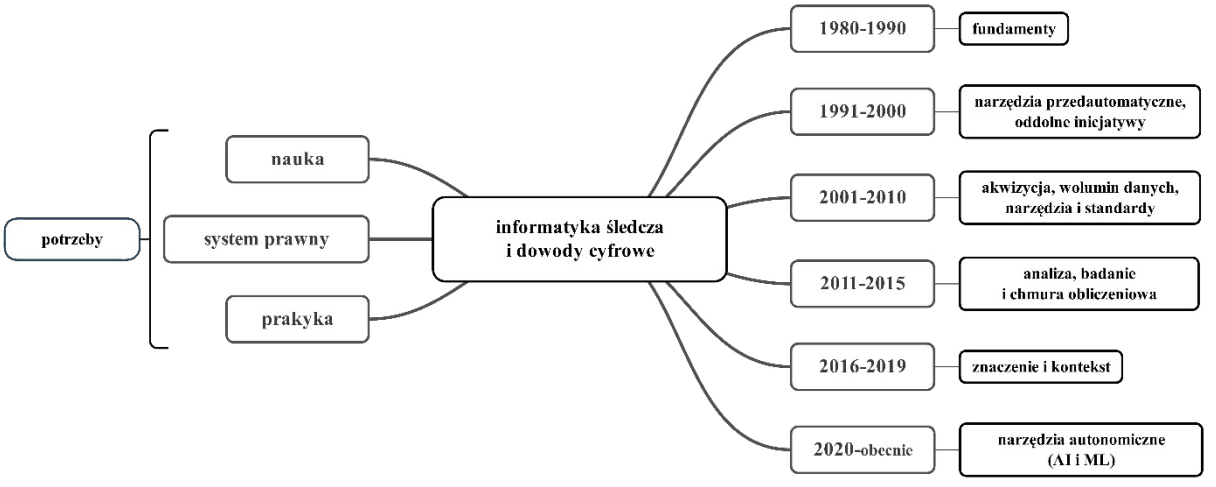
W przyszłości warto by rozważyć – wykorzystując dorobek tej teorii – redefinicję „miejsc szczególnego zagrożenia przestępczością na tle seksualnym", wprowadzonych Ustawą z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie (por. art. 3 pkt 1 ust. 3 oraz art. 22). Wówczas cyberprzestrzeń, a nawet konkretne platformy czy strony internetowe byłyby objęte monitoringiem. Podobnego rozwiązania można dopatrywać się w inicjatywie pod nazwą *Interpol 'Worst Of' List* (IWOL) (OCCRP, 2023; Interpol 2023, 2024).

Informatyka śledcza zorientowana na CSAEM i OCSAE

Z uwagi na ograniczony charakter artykułu w tej części omówiono jedynie wybrane obszary, które będą jeszcze rozwijane przez Autora. Informatyka śledcza – chociaż bywa wciąż opisywana jako „młoda dyscyplina" – liczy sobie około pół wieku. Zgodnie z metaanalizą, której wizualizację przedstawiono poniżej (rys. 5), przeprowadzoną na potrzeby opracowania encyklopedycznego, dziedzina ta weszła niedawno w szósty etap rozwoju:

Rys. 5.

Etapy rozwoju informatyki śledczej i dowodów cyfrowych (opracowanie własne na podstawie: Rogers i in., 2023, s. 10)



Zarówno sama informatyka śledcza, jak i poszczególne jej procesy – np. gromadzenie, zabezpieczanie, analiza danych (Casey, 2010; Szmit, 2014; Kowalski, Radziszewski, 2017; Chojnowski, 2024; Oettinger, 2024) – a także zagadnienia związane z dowodami cyfrowymi (Kasprzak, 2015; Caianiello i in., 2021; Lewulis, 2021; Solanke, 2022) mają bogatą literaturę przedmiotu. Na potrzeby tego tekstu ich ponowne opisywanie wydaje się niezasadne. Stosunkowo niedawno zaczęto pochylać się jednak nad nowymi zagadnieniami, takimi jak: „zeznania maszyny" w sali sądowej (Roth, 2017; Gless, 2020; Dolniak, 2024) czy zależności konstrukcji dowodu cyfrowego od osoby analityka lub biegłego i jego aktywności (Demidova, 2021; Stoykova, 2021; Sunde, 2022).

W kontekście zwalczania CSAEM i OCSAE skupiono się na trzech modelowych procesach: przetwarzaniu – analizie – klasyfikacji (roboczo określanych jako model PAK). Każdy z nich, chociaż w praktyce pełne rozdzielenie nie jest możliwe, również posiada bogatą literaturę fachową (Lee, 2020; Macilotti, 2020; Kumar, 2021; Krać-Batyra i in., 2025; Kamar i in., 2025), a nawet podręczniki (Ferraro i in., 2005; Martelozzo, 2012; Quayle i in., 2012; Elshenraki, 2021). Badania NASK PIB/IWS (na próbie 220 postępowań karnych, zakończonych prawomocnymi wyrokami w latach 2020–2022) wykazały, że w ramach polskiego procesu karnego przetwarzanie, analiza i klasyfikacja CSAEM jeszcze do niedawna miały niesystemowy charakter (np. brak wspólnych dla całego kraju procedur procesowych, brak standardów

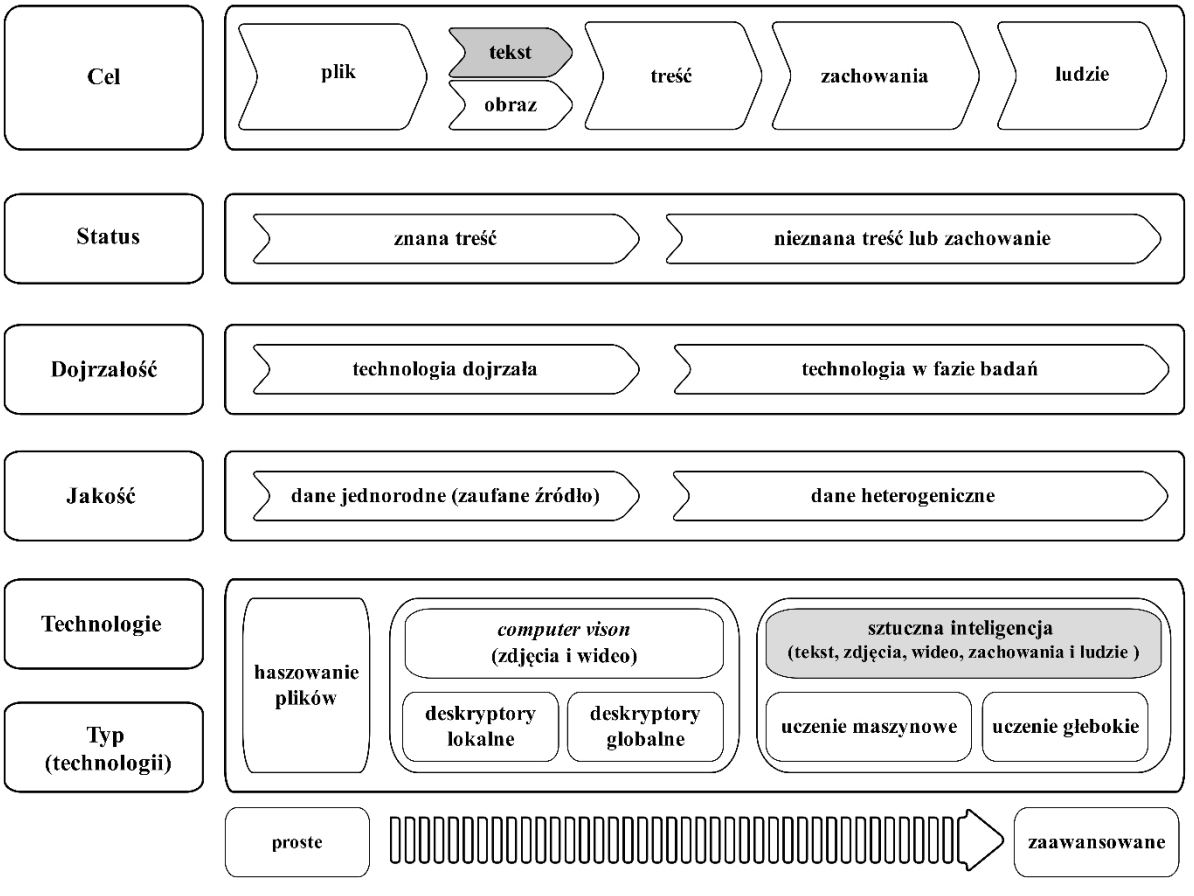
w zakresie narzędzi i metod badawczych). Tymczasem zwalczanie CSAEM i OCSAE wymaga stosowania ujednoliconych procedur oraz dedykowanych rozwiązań teleinformatycznych dostosowanych do potrzeb kraju lub organizacji, w których zostały wdrożone.

Kończąc ten wątek, nie sposób nie wspomnieć o tym, że istnieją ponadto badania dotyczące dostosowanych do analizy i klasyfikacji CSAEM rozwiązań z zakresu informatyki śledczej, których producenci uwzględnili ochronę operatorów oprogramowania (np. analityków, biegłych, prokuratorów) poprzez zadbanie o ich dobrostan (ang. *wellbeing*) czy też redukcję ekspozycji na treści przedstawiające seksualne wykorzystywanie dzieci (Seigfried-Spellar, 2018; Sanchez, i in, 2019; NASK, 2019; Strickland i in., 2023).

W doborze omawianych w dalszej części technologii uwzględniono narzędzia, które cechuje względna autonomiczność (np. bazy CSAM, *crawlery* i *scrapery*), pozwalające m.in. na korelację ze sobą różnorodnych danych – np. plików, metadanych, klasyfikacji – w celu nadania im właściwego znaczenia i kontekstu relewantnego z punktu widzenia m.in. czynności operacyjno-rozpoznawczych czy dochodzeniowo-śledczych.

Celem artykułu nie jest ani stworzenie wyczerpującego katalogu dostępnych narzędzi, ani formułowanie subiektywnych rekomendacji, lecz przedstawienie reprezentatywnych przykładów ilustrujących skalę, różnorodność oraz kierunki rozwoju współczesnych rozwiązań technologicznych wspierających organy ścigania i wymiar sprawiedliwości. Zaprezentowane przykłady służą operacjonalizacji zaktualizowanego przez Autora (obszary wyróżnione kolorem szarym) modelu teoretycznego (rys. 6), zaproponowanego w raporcie pt. *Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse*.

Rys. 6.
Wykrywanie CSAEM i OCSAE – perspektywa technologiczna (opracowanie własne na podstawie: Lazarus i in., 2021, s. 11).



Słowem komentarza należy krótko objaśnić powyższą grafikę. W porządku horyzontalnym określono stopnie złożoności rozwiązań technologicznych (proste > zaawansowane). Na porządek wertykalny składa się sześć analizowanych obszarów (od góry):

1. Cel (inaczej: przedmiot analizy): plik > tekst lub obraz > treść (tekstu/obrazu) > zachowania > ludzie.
2. Status (treści *CSAEM*): znana treść > nieznana treść (lub zachowanie).
3. Dojrzałość (technologii): technologia dojrzała > technologia w fazie badań.
4. Jakość (danych wejściowych): dane jednorodne (z zaufanego źródła) > dane heterogeniczne.

5. Technologie: haszowanie plików > *computer vison* (zdjęcia i wideo) > sztuczna inteligencja (teksty, zdjęcia, wideo, zachowania i ludzie).
6. Typ (technologii): haszowanie plików > deskryptory globalne > deskryptory lokalne > uczenie maszynowe (ang. *machine learning*) > uczenie głębokie (ang. *deep learning*).

Zanim przejdziemy do poszczególnych technologii, krótko podsumujmy: CSAEM oraz OCSAE jako zorganizowana, transgraniczna cyberprzestępczość wymusza wdrożenie skutecznego systemu zwalczania obecnych (zob. trendy opisywane m.in. w raportach Dyżurnet.pl, 2024, 2025) i rozpoznawania nowych działań przestępczych naruszających prawo (NPCC, 2025; UK.GOV, 2025; CameraForensics, 2025). System (czy też systemy), choćby najlepiej pomyślane na poziomie organizacyjnym (ECPAT, 2025b; OOSI, 2022) czy finansowym (Safeguarding Childhood, 2025), nie będą skuteczne bez wykorzystania dwóch – wskazanych w powyższej tabeli – technologii: algorytmów haszujących oraz detektorów CSAEM opartych o sztuczną inteligencję.

Algorytmy haszujące

Według INHOPE (INHOPE, 2025c) rok 2024 był najtrudniejszym w historii działalności sieci *hotline'ów* zrzeszonych w tej organizacji. Wykryto wtedy około 2,5 mln rekordów zawierających potencjalne CSAEM, przy czym pojedynczy rekord może zawierać jeden lub nawet kilka tysięcy plików. Oznacza to ponad 200% wzrost w stosunku do poprzedniego roku raportowego. Thorn (Thorn, 2023) alarmuje, że NCMEC w 2023 r. zaraportował 104 mln plików przedstawiających seksualne wykorzystywania dzieci (w 2017 r. było ich 20 mln).

Algorytmy haszujące – czy to w postaci haszy kryptograficznych czy też tzw. haszy inteligentnych – stanowią podstawową technologię, od lat używaną w informatyce śledczej (Breitinger i in., 2013; McKeown i in., 2019) oraz zwalczaniu cyberprzestępczości (García-Retuerta i in., 2019; Farid, 2018; Ofcom, 2022), w tym również w walce z CSAEM i OCSAE (Interpol, 2018; Daskalaki i in., 2025).

Algorytmy takie jak np. MD5, SHA-1, SHA-256 pozwalają szybko i jednoznacznie stwierdzić identyczność porównywanych danych wejściowych (np. dwóch plików przedstawiających wizerunek osoby). Dwa pliki, dla których wyliczono hasz o identycznej wartości (np. MD5: 6d6fdd8e1c0527d45fb2534a29c2ae32), są na poziomie binarnym, tj. z dokładnością co do jednego bitu, identyczne. Jedną z większych zalet takiego rozwiązania, oprócz niewątpliwej jego szybkości, jest możliwość stwierdzenia całkowitej zgodności treści bez otwierania i oglądania plików.

Hasze tzw. inteligentne (np. PhotoDNA, ZZ40, PDQ, NeuralHash, Videntifier) umożliwiają stwierdzenie podobieństwa wizualnego (treściowego) plików. To rozwiązanie powala wykazać poziom zgodności występujący pomiędzy materiałem weryfikowanym (plik A – np. kolorowe zdjęcie przedstawiające wizerunek osoby małoletniej w ubraniu) oraz materiałem referencyjnym, który – po uprzedniej klasyfikacji i kategoryzacji – został umieszczony w bezpiecznym i wiarygodnym repozytorium, takim jak baza CSAM (plik B – np. czarno-białe zdjęcie przedstawiające wizerunek osoby małoletniej bez odzieży). Tego typu hasz (Farid, 2021; Morales i in., 2024) pozwala wykrywać serie podobnych materiałów (np. przekonwertowanych na skalę szarości, przyciętych czy zrotowanych) albo też zdjęcie/wideo przedstawiające podobne pomieszczenia czy osoby w innych kontekstach wizualnych.

Z uwagi na szybkość, a także względną prostotę rozwiązań opartych na haszach wdrożyły je służby, organizacje i podmioty komercyjne na całym świecie (np. Interpol, Europol, australijski Argos, VIC Project, Pathfinder; NCMEC, IWF, C3P, Google, Facebook, YouTube, WhatsApp, Instagram).

Wybrane dane dotyczące przykładowych międzynarodowych bazy haszy mówią same za siebie. NCMEC, który powstał w 1984 r., dysponuje bazą około 10 mln potrójnie zweryfikowanych wartości hasz. Interpolowa baza treści CSAM – w latach 2001–2008 działająca jako *Child Abuse Image Database*, a w 2009 r. przekształcona w *ICSE Database* – przechowuje i przetwarza obecnie około 5 mln plików (zdjęć i wideo). Szacuje się, że istniejąca od około 20 lat europolowa baza *IVAS* jest znacznie większa (brak na chwilę obecną dokładnych informacji). Baza *Project VIC US* (działa od 2013 r.) dysponuje około 19 mln wartości hasz.

W odniesieniu do ww. baz warto zaznaczyć, że żadna z nich nie jest w pełni zgodna z polską legislacją. Obecnie brak krajowego systemu agregacji danych (plików oraz haszy), a także informacji o CSAEM (np. klasyfikacja i kategoryzacja). Polskie organy ścigania (głównie Wydział Do Walki Z Handlem Ludźmi Biura Kryminalnego KGP oraz Centralne Biuro Zwalczania Cyberprzestępczości), w celu realizacji rozproszonych pomiędzy sobą zadań związanych z ochroną dzieci przed przestępczością seksualną w cyberprzestrzeni, od lat korzystają zarówno do czynności operacyjnych, jak i procesowych z większości tych – co warto wyraźnie podkreślić: nie w pełni kompatybilnych z naszym Kodeksem karnym – rozwiązań.

Wszelkie wykorzystywane niepolskie zestawy haszy (np. *VIC Project*, *ICSE*, *IVAS*) mogą posłużyć jedynie do filtrowania znanych (według różnych systemów klasyfikacji i kategoryzacji tworzonych w oparciu o zagraniczne prawo karne) plików. W efekcie obecny mechanizm wykorzystania zagranicznych haszy sprawia, że cały zbiór danych audiowizualnych i tak musi zostać przejrzany manualnie w celu selekcji

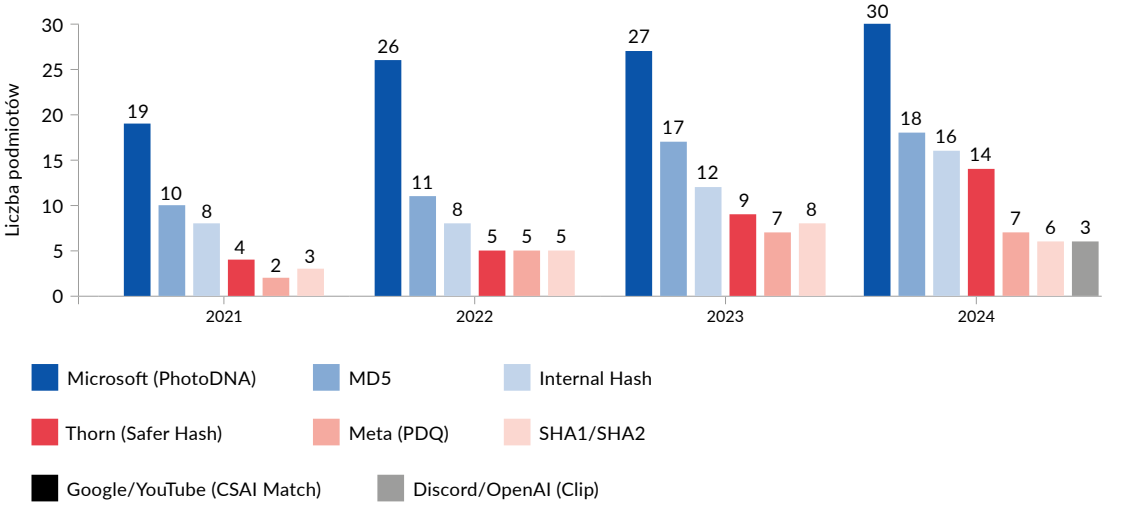
treści relewantnych dla polskiego Kodeksu karnego. Obciąża to system karny zarówno w zakresie czasu (manualne przeglądanie trwa nieporównywalnie dłużej niż działanie programu wykorzystującego wartości hasz), jak i kosztów osobowych czy finansowych.

Potencjał haszy w walce z CSAEM i OCSAE zależy w dużej mierze od możliwości ich agregacji, szybkiego przetwarzania i walidowanej jakości danych (m.in. jednorodnej kategoryzacji zgodnej z krajową legislacją). Systemy teleinformatyczne (zazwyczaj zcentralizowane bazy haszy i wizerunków), zapewniające wielopoziomowe bezpieczeństwo przetwarzania, pozwalają w sposób zautomatyzowany wykonywać miliardy operacji bez obciążania tym zadaniem człowieka (Brown, i in, 2018; CLKP, 2018; Kemal, 2019; UK.GOV, 2024; Google, 2026).

Efektywność automatyzacji całego procesu można przedstawić na przykładzie Google'a (Google, 2026). W pierwszej połowie 2025 r. na ponad 3 mln (3 124 107) zgłoszeń dotyczących CSAEM (każde z nich mogło obejmować zarówno pojedyncze zdjęcie, jak i ich wielotysięczny zbiór, konto czy nawet stronę internetową) manualnie przetworzono ich zaledwie 13 526, a w sposób zautomatyzowany (w tym z wykorzystaniem haszy i AI) – 3 110 581. Referencyjne bazy haszy i wizerunków pozwalają na szybką i skuteczną detekcję, blokowanie (ograniczenie dostępu publicznego) i usuwanie (trwałe nadpisywanie pamięci dyskowej). Dlatego korzystają z nich dostawcy usług internetowych, w tym platformy współpracujące w ramach TechCoalition (rys. 7a–b). Warto ponownie odnotować, że z uwagi na liczbę treści CSAEM, rokrocznie raportowanych przez niektórych usługodawców, a także częstotliwość występowania w ich usługach OCSAE mogą być one rozpatrywane w ramach wspomnianej *lawless space theory*.

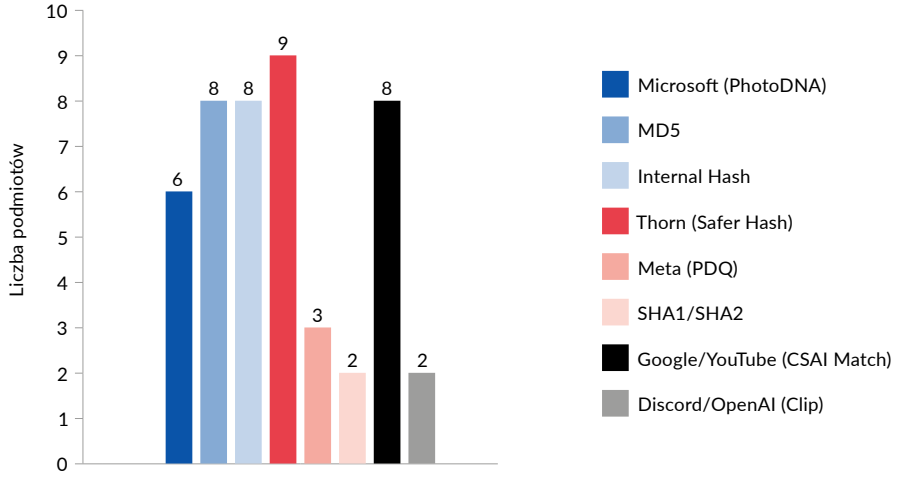
Rys. 7a.

Wykorzystanie haszy do filtrowania zdjęć w latach 2021–2024 (opracowanie własne na podstawie: TechCoalition, 2025c, s. 28)



Rys. 7b.

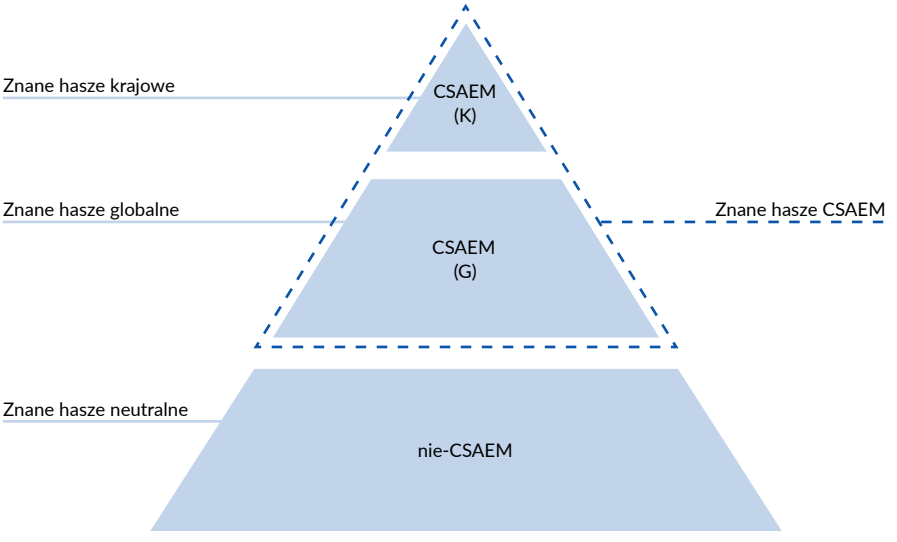
Wykorzystanie haszy do filtrowania wideo (2024) (opracowanie własne na podstawie: TechCoalition, 2025c, s. 29)



Najważniejszą zaletą wiarygodnego zbioru haszy jest szybkie odfiltrowanie znanego CSAEM od tego, którego jeszcze nie ma w bazie. Ta druga kategoria

automatycznie uzyskuje wyższy priorytet podejmowanych działań, np. zgłoszenie do odpowiednich organów ścigania lub przekazanie do zespołów właściwych do spraw identyfikacji osób pokrzywdzonych (ang. *victim identification*, VID). Pliki, których jeszcze nie skategoryzowano jako CSAEM (brak ich haszy w bazie), mogą bowiem przedstawiać osobę małoletnią zagrożoną – chociażby w czasie odpytywania bazy – przestępstwem seksualnym. Zależność między zbiorami haszy można zwizualizować następująco (rys. 8).

Rys. 8.
Podział haszy według typu (znane neutralne – znane globalne – znane krajowe) (opracowanie własne)



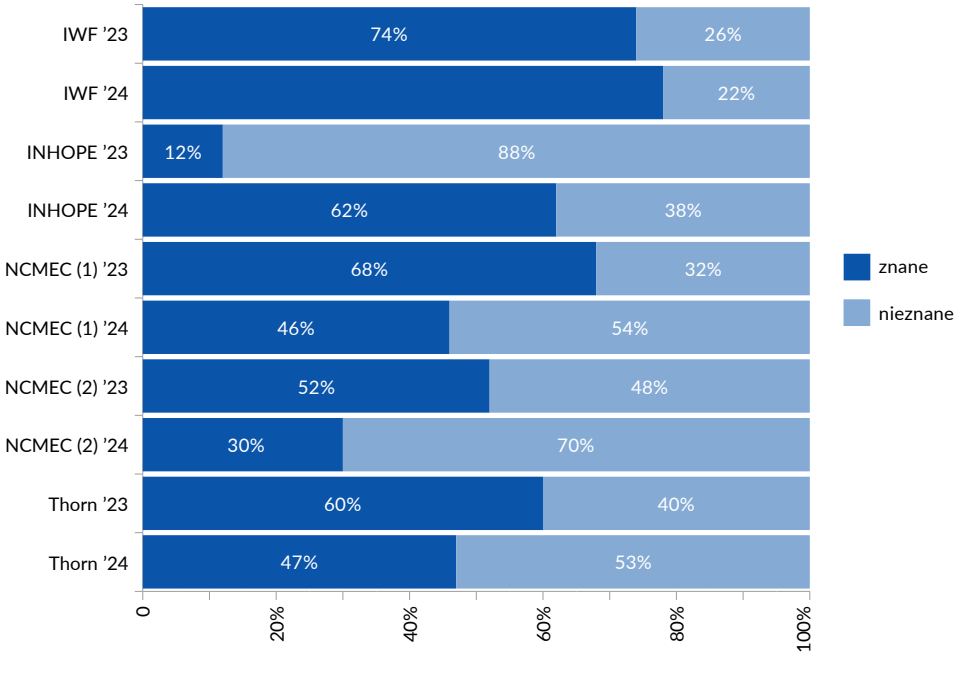
Przykładem wymienionych w dolnej części piramidy haszy neutralnych (nie-CSAEM) o zasięgu międzynarodowym mogą być powszechnie dostępne zbiory NIST NSRL oraz komercyjny HashSets.com. Amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) to federalna agencja działająca w strukturze Departamentu Handlu (DOC U.S.), odpowiedzialna za opracowywanie standardów z zakresu technologii czy cyberbezpieczeństwa. *National Software Reference Library* (NSRL) to z kolei aktualizowany na bieżąco zbiór zawierający hasze referencyjne plików uznawanych za znane i nieszkodliwe. Podzbiór *Reference Data Set* (wersja 3) liczy obecnie 552 038 839 haszy (NIST, 2026). HashSets.com również oferuje skumulowany zasób unikalnych wartości haszy. W podzbiorze *White Hash Set* znajdują się hasze znanych plików, które uznano za bezpieczne lub nieszkodliwe. Baza ta w latach 2015–2025

zanotowała blisko czterokrotny wzrost: z 24 063 530 do 89 234 821 rekordów (HashSets.com, 2026).

Poniższa grafika (rys. 9) pozwala zrozumieć, jak w poszczególnych organizacjach zajmujących się zwalczaniem OCSAE (tu: IWF, INHOPE, NCMEC oraz Thorn) wygląda zautomatyzowana detekcja treści z perspektywy podziału na nowe (nieposiadające wartości hasz w bazie tej organizacji) oraz znane (tj. wcześniej przeanalizowane przez tę organizację). NCMEC został wymieniony dwukrotnie, ponieważ w opracowaniu źródłowym podano zestawienie treści znanych z nieznanymi ze względu na dwie różne technologie, tj. hasze inteligentne pozwalające wykrywać podobieństwo obrazów (ang. *visually similar images*) oraz hasze kryptograficzne pozwalające wykrywać obrazy identyczne (ang. *exact images maches*). Nie jest to przedmiotem niniejszej analizy i zainteresowanych czytelników odsyłamy do cytowanego artykułu, jednak warto zauważyć, że dopasowanie na poziomie podobieństwa może znacząco redukować liczbę nieznanych treści.

Rys. 9.

Status treści CSAEM według kryterium znany/nieznany hasz w latach 2023–2024 (opracowanie własne na podstawie: Childlight, 2025a, s. 64–65)



Na koniec tej części warto jeszcze dodać, że międzynarodowe bazy CSAM (haszy i wizerunków) stanowią zbiór danych bardzo niejednorodnych, a ich wykorzystanie – niezbędne do efektywnej detekcji takich treści – każdorazowo powinno być poprzedzone dokładną analizą potrzeb i dobrze zaplanowanym procesem wdrożenia, gdyż:

> tworzono je w celu wsparcia krajowych lub regionalnych organów ścigania, a te z kolei posiadają własne regulacje prawne, definiujące m.in. instytucje dziecka czy karalnych czynności seksualnych (Krać-Batyra i in., 2025, s. 66).

Korelacja oraz interoperacyjność zasobów znajdujących się w międzynarodowych bazach CSAM w sposób umożliwiający wzajemne wykorzystanie klasyfikacji, haszy czy nawet plików stanowi obecnie jedno z większych wyzwań. Dlatego też od lat podejmowane są różnego rodzaju inicjatywy, które można podzielić zasadniczo na dwie grupy.

Z jednej strony istnieją projekty i technologie integrujące, tj. GRACE, AVIATOR, IntelliGrade czy The Universal Classification Schema (GRACE, 2020; AVIATOR, 2024; EU Funding, 2025; IWF, 2025; INHOPE, 2025b), do których dołączyła również TechCoalition, realizująca projekty Lantern oraz VHIP/The Alpha (TechCoalition, 2023, 2025a; Chau, 2022).

Można tu także zaliczyć badania porównawcze w postaci kompleksowych przeglądów mechanizmów detekcji stosowanych przez platformy internetowe. Jedno z takich badań po raz drugi zostało przygotowane przez wspomniany już OECD (OECD, 2023, 2025). Obejmuje ono 50 platform internetowych (m.in. Facebook, YouTube, WhatsApp, Instagram, TikTok, Snapchat, czy Discord). W przejrzystym, tabelarycznym zestawieniu przedstawiono metody (np. algorytmy haszujące, zgłoszenia użytkowników, weryfikacja przez personel, bazy adresów URL, narzędzia oparte na sztucznej inteligencji oraz interfejsy API) stosowane w danej usłudze w celu wykrywania CSAE.

Polska – opracowując ramy legislacyjne dla krajowego systemu baz CSAM (Kancelaria Prezesa Rady Ministrów, 2025; CyberDefence24, 2025) – wpisuje się w drugi nurt. Państwa, które posiadają doświadczenie we współpracy międzynarodowej, a także osiągnięcia w walce z CSAEM i OCSAE, udoskonalają system rozwiązań krajowych czy to poprzez tworzenie krajowych baz haszy i wizerunków (np. Szwecja, Niemcy, Rumunia), czy też poprzez rozwój modeli AI do detekcji treści penalizowanych właśnie w tym kraju (wspomniany już ODIP we Francji czy polski APAKT).

Sztuczna inteligencja

Przegląd (Wolbers i in., 2025) zastosowań sztucznej inteligencji w obszarze zwalczania OCSAE wskazuje, że rozwiązania te obejmują całe spektrum funkcji: od automatycznego wykrywania materiałów CSAEM na podstawie nazw plików, ścieżek dostępu oraz analizy obrazu i wideo, przez preklasyfikację treści, szacowanie wieku małoletnich, identyfikację sprawców (ang. *perpetrator identification*, PID) oraz osób pokrzywdzonych (VID) z wykorzystaniem rozpoznawania twarzy i głosu, aż po analizę języka i zachowań w środowisku cyfrowym w celu wykrywania (nowych) zagrożeń, profilowania sprawców oraz monitorowania aktywności przestępczej w darknecie.

Skuteczne wykorzystanie AI do detekcji CSAEM i OCSAE wymaga dobrze przygotowanego zbioru danych treningowych (Ramesh Babu, 2024; Wilkowski, 2025; Macedo i in. 2025). Modele do detekcji pornografii czy nagości, mimo pewnego stopnia przydatności, nie powinny być wykorzystywane do automatyzacji prekategoryzacji CSAEM. Jak zauważono w cytowanym raporcie OECD:

> Identyfikowanie wcześniej nieznanych treści przedstawiających seksualne wykorzystywanie dzieci lub wykrywanie podejrzanych zachowań w sieci stanowi jedno z większych wyzwań dla moderacji treści opartej na technologiach. Wykorzystanie sztucznej inteligencji i uczenia maszynowego w tym obszarze podlega stałemu rozwojowi. Identyfikacja potencjalnie nielegalnych treści zazwyczaj opiera się na algorytmach klasyfikujących oraz rozpoznawaniu wzorców. Z natury rzeczy technologie te nie są tak dokładne i – aby poprawić swoją skuteczność – wymagają trenowania na dużych zbiorach danych (OECD, 2023, s. 26).

Takim *datasetem* do wytrenowania skutecznego modelu AI, służącego do identyfikacji materiałów uznanych w Polsce za nielegalne, może być krajowa baza CSAM, zawierająca przykładowo jedną kategorię (inaczej zbiór) danych – np. treści przedstawiające seksualne wykorzystywanie dzieci. Kategorię tę należałoby nadać wszystkim materiałom audiowizualnym, których kwalifikacja prawna jest zgodna z obowiązującą w Polsce legislacją. Każdy plik, który trafi w bazie CSAM do kategorii „nielegalne", powinien w pierwszej kolejności zostać w pełni sklasyfikowany (np. zgodnie z *Universal Classification Schema*).

W tym miejscu pochylimy się nad prawidłowym zmapowaniem najważniejszych pojęć. Klasyfikacja treści jest procesem wykonywanym przez osobę posiadającą odpowiednią wiedzę i doświadczenie odnośnie do percepcji, selekcjonowania oraz (w razie potrzeby) opisywania CSAEM. W Polsce takie umiejętności i wiedzę

specjalistyczną posiadają np. biegli z zakresu badań antropologicznych czy seksuologicznych oraz specjaliści Dyżurnet.pl NASK PIB.

Warto nadmienić, że zgodnie z art. 193 k.p.k. biegły powinien być włączany do procesu karnego jedynie wtedy, kiedy „stwierdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy wymaga wiadomości specjalnych". Natomiast dla pewnego zbioru danych CSAEM, do stwierdzenia, że przedstawiają one dziecko podczas czynności seksualnej, wystarczą m.in. „doświadczenie życiowe i zakres wiedzy ogólnej" (por. wyrok SN z dnia 15.04.1976 r. IIKR 48/76, OSNKW 1976, nr 10–11, poz. 133).

W ramach klasyfikacji określa się m.in., czy na zdjęciu widoczna jest osoba małoletnia i czy bierze ona udział w czynności seksualnej. Atrybut małoletniości do pewnego wieku – a precyzyjniej rzecz ujmując: do pewnego widocznego na materiale wizualnym etapu rozwoju – jest tzw. faktem notoryjnym. Przykładowo: nie do zakwestionowania jest małoletniość dziecka w wieku niemowlęcym. Szacowanie odbywa się na podstawie dających się stwierdzić naocznie wtórnych (drugo- i trzeciorzędowych) cechy płciowych. Podobne zasady należy przyjąć w odniesieniu do pewnej grupy czynności seksualnych (np. penetracja waginalna czy oralna).

Klasyfikacji (zwłaszcza dla pewnej grupy CSAEM) można przypisać atrybut obiektywności oraz irrelewantności w odniesieniu do kwalifikacji prawnej. Klasyfikacja nie musi być opisowa, jednakże w niektórych przypadkach (np. na potrzeby przygotowania materiału przez/dla seksuologa) może być pożądana. Zazwyczaj wystarczy oznaczenie tzw. tagiem lub etykietą (ang. *label*) czy też zakodowanie informacji w inny sposób, określony w systemie klasyfikacji. Przykładowo: użycie ustandaryzowanego kodowania alfanumerycznego z dwoma typami znaków (cyfry arabskie, duże litery) może zawierać informację o liczbie osób widocznych na zdjęciu (np. 2P) oraz ich płci (2M), a także kategorii wiekowej (A, C). Zapis w postaci '2P, 2M, A, C' może więc oznaczać dwie osoby (ang. *person*, tu: P), płci męskiej (ang. *male*, tu: M), z których jeden to dorosły (ang. *adult*, tu: A), a drugi to dziecko (ang. *child*, tu: C). Więcej o wykorzystaniu deskrypcji w analizie i klasyfikacji treści znajduje się w dalszej części artykułu.

Natomiast kategoryzacja polega na włączeniu materiału audiowizualnego – na podstawie klasyfikacji jego treści (lub rzadziej w oparciu o metadane) – do arbitralnie wyodrębnionej grupy, np. legalne/nielegalne czy istotne/nieistotne dowodowo (por. wcześniejszą informację o zestawach haszach neutralnych). Co do zasady, kategoryzacja powinna być skorelowana z kwalifikacją prawną relewantną dla danego zbioru danych, np. krajowej bazy CSAM.

W zakończeniu tej części przedstawiono badanie TechCoalition (TechCoalition, 2025b, s. 31), istotne chociażby z perspektywy opracowywania założeń ww. rozwiązania krajowego. Prześledzono w nim, w jakim celu w ostatnich latach (2022–2024) dostawcy usług internetowych wykorzystywali modele AI (dane przedstawiono według konwencji: rok – liczba podmiotów):

- do klasyfikacji zdjęć (odpowiednio 2024 – 33, 2023 – 21, 2022 – 13);
- wideo (odpowiednio: 2024 – 19, 2023 – 10, 2022 – 4);
- do klasyfikacji *groomingu* (odpowiednio: 2024 – 8, 2023 – 10, 2022 – 9);
- *sextortion* (odpowiednio: 2024 i 2022 – 4, 2023 – 5).

Oprogramowanie do informatyki śledczej zorientowanej na CSAEM i OCSAE

Jak już wspomniano w niniejszym artykule, coraz częściej opracowywane są badania dotyczące dobrostanu osób na co dzień przetwarzających, analizujących i klasyfikujących treści CSAEM. Przykładowo w Wielkiej Brytanii zwraca się uwagę na rolę informatyków śledczych, wspierających lokalne i krajowe organy ścigania w walce z tym zjawiskiem, którego stały wzrost obserwowany jest tam od lat dziewięćdziesiątych XX w.:

> (…) specjalistyczne jednostki policji zostały zaprojektowane w celu reagowania na to zagrożenie, a pełniący w nich służbę wyspecjalizowani funkcjonariusze (określani w Wielkiej Brytanii jako analitycy informatyki śledczej) badają zabezpieczone w ramach dochodzeń (ang. *police investigation*) urządzenia elektroniczne pod kątem obecności CSAEM. W Wielkiej Brytanii wiąże się to z ręcznym przetwarzaniem wszystkich „nieznanych" materiałów cyfrowych (tj. takich, które nie są „znane" brytyjskiej bazie danych obrazów wykorzystywania dzieci – *Child Abuse Image Database* (…). Analitycy informatyki śledczej, wykonując swoje codzienne obowiązki służbowe, są więc rutynowo narażeni na kontakt z CSAEM (Strickland i in., 2023, s. 2).

W jednym z nowszych badań (Tselenti i in., 2025) na temat wyzwań zawodowych, z jakimi mierzą się funkcjonariusze organów ścigania (tu: w Niemczech, Portugalii i Szwecji) podczas prowadzenia postępowań w sprawach dotyczących CSAEM i OCSAE, zidentyfikowano bariery organizacyjne, takie jak nadmierne obciążenie pracą, braki kadrowe oraz trudności w zarządzaniu ogromną ilością materiałów cyfrowych (por. etapy rozwoju informatyki śledczej).

Autorzy uchwycili także istotne problemy systemowe, w tym ryzyko wtórnej wiktymizacji pokrzywdzonych (wynikającej z wielokrotnego oglądania przez różnych

funkcjonariuszy tego samego materiału dowodowego – czy to w obrębie różnych postępowań w danej jednostce, czy w różnych jednostkach w skali kraju) oraz niespójne przepisy prawne utrudniające skuteczne ściganie sprawców. Zwrócono tam również uwagę na zagadnienia związane z technologią:

> W świetle rosnącego stopnia zaawansowania przestępstw cyfrowych (...) uczestnicy podkreślali znaczenie bycia technologicznie „na bieżąco". Postrzegali sprawców, którzy działają w internecie, jako osoby stale udoskonalające swoje metody uzyskiwania dostępu do CSEM i jego rozpowszechniania: „często ma się do czynienia z ludźmi, którzy są niesamowicie biegli w IT, więc zawsze trzeba za nimi nadążać" (...). W konsekwencji niektórzy uczestnicy wyrażali obawy dotyczące możliwego braku zaawansowanego sprzętu komputerowego i umiejętności, co sprawiało, że czuli się technologicznie nieprzygotowani do skutecznego prowadzenia dochodzeń dotyczących OCSAE (Tselenti i in., 2025, s. 7).

W dalszej części zostaną wymienione (tabela 2) i omówione technologie i narzędzia, które – w kontekście przetwarzania, analizy i klasyfikacji treści przedstawiających seksualne wykorzystywanie dzieci w cyberprzestrzeni – są dostępne od wielu lat (Sanchez, 2019, s. 135), lub takie, które mogą zostać wprowadzone w najbliższym czasie (m.in. APAKT, CPORT, Arthropod).

Tabela 2.

Narzędzia wykorzystywane przez biegłych/analityków w pracy z treściami CSAEM (opracowanie własne na podstawie: Sanchez i in. 2019, s. 135)

Oprogramowanie	do przetwarzania obrazu		do przetwarzania wideo	
	Liczba	%	Liczba	%
Analyze 16.1 / Griffeye	54	10,07	52	11,79
Autopsy	21	3,92	11	2,49
Cellebrite Analytics	23	4,29	16	3,63
Celebrite UFED/PA	88	16,42	74	16,78
CAINE	6	1,12	3	0,68
Digital Forensics Framework (DFF)	1	0,19	2	0,45
EnCase Forensics	59	11,01	50	11,34
EnCase Mobile Investigartor	8	1,49	6	1,36
Forensics Toolkit (FTK)	64	11,94	56	12,70
Magnet Forensics IEF / Axiom	87	16,23	78	17,69
NuDetective	1	0,19	nie dotyczy	nie dotyczy
Oxygen Forensics Analysis	10	1,87	8	1,81
Oxygen Forensics Detective	10	1,87	8	1,81
Paraben E3: DS	1	0,19	1	0,23
Paraben E3: Universal	1	0,19	1	0,23

Oprogramowanie	do przetwarzania obrazu		do przetwarzania wideo	
	Liczba	%	Liczba	%
PhotoDNA	21	3,92	13	2,95
PlainSight	1	0,19	1	0,23
The SleuthKit	11	2,05	7	1,59
VizX2/ZiuZ	1	0,19	1	0,23
X-Ways Forensics	45	8,40	35	7,94
Inne	22	4,10	16	3,63

Oprogramowanie do zastosowań ogólnych

Przykład 1. Autopsy

Autopsy[5] to narzędzie typu *open source*, którego twórcą jest Brian Carrier. Program towarzyszy informatykom śledczym na całym świecie od ponad 20 lat w wersji *command line* (The Sleuth Kit) oraz w wersji z interfejsem graficznym (GUI). Dzięki rozbudowanym modułom może posłużyć do analizy większości desktopowych systemów operacyjnych (Windows, Linux macOS), urządzeń mobilnych (wybranych), a także różnego rodzaju danych (pamięć RAM, treści multimedialne).

Wśród funkcji Autopsy, które mogą okazać się przydatne do przetwarzania, analizy i klasyfikacji CSAEM, warto wymienić rozpoznawanie i odzyskiwanie znacznej liczby formatów multimedialnych, wyszukiwanie na podstawie słów kluczowych czy badanie artefaktów związanych z aktywnością w internecie oraz korzystaniem z P2P.

Autopsy należy do grupy programów ogólnego zastosowania w informatyce śledczej, które pozwalają na identyfikację znanych plików w oparciu o bazę haszy kryptograficznych (np. MD5, SHA-1) i perceptualnych. Rozwiązaniem skierowanym do osób wykonujących czynności techniczne z CSAEM (bez dostępu do innych narzędzi) jest pakiet *Law Enforcement Bundle* (zawierający moduły Project VIC oraz C4P), który umożliwia automatyczną identyfikację i kategoryzację (według amerykańskiego systemu prawnego) znanych materiałów w oparciu o aktualizowane dane z *Project VIC*, czy też korzystanie z bazy haszy do deduplikacji materiałów przedstawiających seksualne wykorzystywanie dzieci.

Przykład 2. X-ways Forensics Professional

X-Ways Forensics to jedno z komercyjnych rozwiązań autorstwa Stefana Fleischmanna (X-Ways Software Technology AG), rozwijanych od blisko 30 lat.

5 Obecnie program w wersji 4.22.1 (kwiecień 2025) wraz z dodatkowymi modułami dostępny jest na stronie: https://www.autopsy.com; dodatkowe informacje, w tym historię rozwoju oprogramowania, można uzyskać na stronie: https://www.sleuthkit.org/autopsy/history.php

Program – obecnie w wersji 21.6 – na stronie producenta (https://x-ways.net/forensics/index-m.html) opisywany jest jako: „zaawansowane środowisko pracy dla biegłych z zakresu informatyki śledczej". Jego przewagą nad konkurencją ma być lepsza wydajność i mniejsze zużycie zasobów, a także większa skuteczność m.in. w wyszukiwaniu słów kluczowych czy też odzysku danych (NIST, 2015; Homeland Security, 2014; Shavers, 2022).

Wymienienie wszystkich możliwości oprogramowania wymagałoby odrębnego opracowania. Szczegółowy podręcznik użytkownika (ang. *manual*) dostarcza producent, a w przypadku potrzeby pogłębienia wiedzy o działaniu i zastosowaniach narzędzia warto sięgnąć do cytowanej publikacji i szkoleń Bretta Shaversa. Natomiast z perspektywy przetwarzania i analizy treści CSAEM warto zwrócić uwagę na kilka funkcji.

X-Ways Forenics, oprócz kilku rozwiązań wymienionych przy okazji Autopsy, posiada bardzo zaawansowaną i niezwykle szybką obsługę wewnętrznej bazy haszy, w tym PhotoDNA. Kolejnym z rozwiązań wspierających analizę treści CSAEM jest rozbudowany moduł odzyskiwania danych, pozwalający na zaawansowaną konfigurację mechanizmu *carvingu* i trybów odzyskiwania o różnej czułości. Dodatkowo program zapewnia wyszukiwanie słów kluczowych i dedykowane filtry artefaktów.

Ostatnim z elementów pozwalających docenić to narzędzie od strony praktycznej jest względna otwartość na innych wytwórców oprogramowania i potrzeby użytkowników. Rozszerzenie funkcji programu możliwe jest za pomocą tzw. *X-Tensions* oraz modułów, które umożliwiają analizę dowodów cyfrowych w zakresie wykraczającym poza typową funkcjonalność programu Fleichmana. W odniesieniu do analizy obrazu są to m.in. moduły związane z monitoringiem CCTV oraz Excire[6] (m.in. analiza offline zdjęć z wykorzystaniem sztucznej inteligencji, w tym w oparciu o prompty). W odniesieniu do ostatniego rozwiązania Autor podaje na swojej stronie (https://x-ways.net/excire.html):

> Excire Forensics to moduł zintegrowany z X-Ways Forensics, oparty na technologii opracowanej przez Pattern Recognition Company GmbH. Excire zapewnia rozszerzenie naszego oprogramowania o (…): automatyczną analizę zdjęć i rozpoznawanie w treści obrazu obiektów, takich jak określone rodzaje budynków, pojazdów, zwierząt (…) ludzie w różnym wieku, nagość i pornografia (…); wyszukiwanie twarzy poszczególnych osób na zdjęciach nowych spraw.

6 Program może być używany jako moduł (https://www.x-ways.net/excire.html; https://excire.com/en/excire-computer-vision-api/) lub niezależne narzędzie działające offline (Excire Foto, 2025).

Po wstępnym przetworzeniu wskazanych plików audiowizualnych oprogramowanie działa błyskawicznie, ponieważ wszystkie informacje znajdują się w specjalnie do tego celu utworzonej bazie danych. Możliwe jest także ich przedstawienie i dalsze filtrowanie, również w oparciu o wcześniej wspomnianą deskrypcję. Poniżej przedstawiono przekładowe zestawienie tabelaryczne (tabela 3), które zawiera istotne z punktu widzenia klasyfikacji CSAEM annotacje (inne nazwy to: tagi, etykiety), np. *child*, *body*, *nude*.

Tabela 3.
Annotacja treści zdjęć przy użyciu X-Tension Excire (opracowanie własne na podstawie: Shavers, 2022, s. 317)

Zestawienie (ang. *raport table***)**
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, bez okularów, oczy otwarte, portret, niebieski
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, bez okularów, oczy otwarte, portret, niebieski, podobny do CNN Larry King
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, bez okularów, oczy otwarte, brązowy
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, czarny kolor, bez okularów, oczy otwarte
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, czarny kolor, bez okularów, oczy otwarte, portret
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, szary, bez okularów, oczy otwarte, chmury, natura, niebo
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, szary, bez okularów, oczy otwarte, znak
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, szary, bez okularów, oczy otwarte, szary kolor, podobny do Larry Kinga z CNN
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, okulary, czarny kolor, portret, podobny do Larry Kinga z CNN
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, dorosły, okulary, biały, oczy otwarte, portret
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, okulary, oczy otwarte, portret, osoba starsza
twarz, widok z przodu, osoba, jedna twarz, bez brody, bez uśmiechu, mężczyzna, okulary, szary, oczy otwarte, osoba starsza, natura, roślina

Oprogramowanie dedykowane do walki z CSAEM i OCSAE

Według wiedzy Autora żadne z dedykowanych narzędzi (np. Griffeye, Videntifier, BlueBear, VisionX, Fenzoz) nie zostało do chwili publikacji wdrożone jako ogólnokrajowe, systemowe rozwiązanie w polskiej Policji.

Nadal w fazie opracowania jest też krajowy system walki z CSAEM. Jego zarys został przedstawiony w *Krajowym Planie Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich na lata 2023–2026* (KPRM,

2023). Realizacja *Krajowego Planu* zakłada przygotowanie i/lub wdrożenie rozwiązań teleinformatycznych pozwalających wykorzystać opisany powyżej potencjał haszy (2.1.12. *Przygotowanie do wdrożenia i wdrożenie systemu wymiany informacji o wartościach* hash *między Policją, NASK PIB/Dyżurnet.pl oraz sektorem prywatnym*). Planowana jest także baza zobrazowań (2.4.2. *Przygotowanie do wdrożenia krajowej bazy materiałów przedstawiających wykorzystywanie seksualne dzieci*). Zgodnie z zakładanym harmonogramem w 2025 r. powinno zostać uruchomione rozwiązanie oparte na haszach, a w 2026 r. – baza zobrazowań (propozycje zmian legislacyjnych).

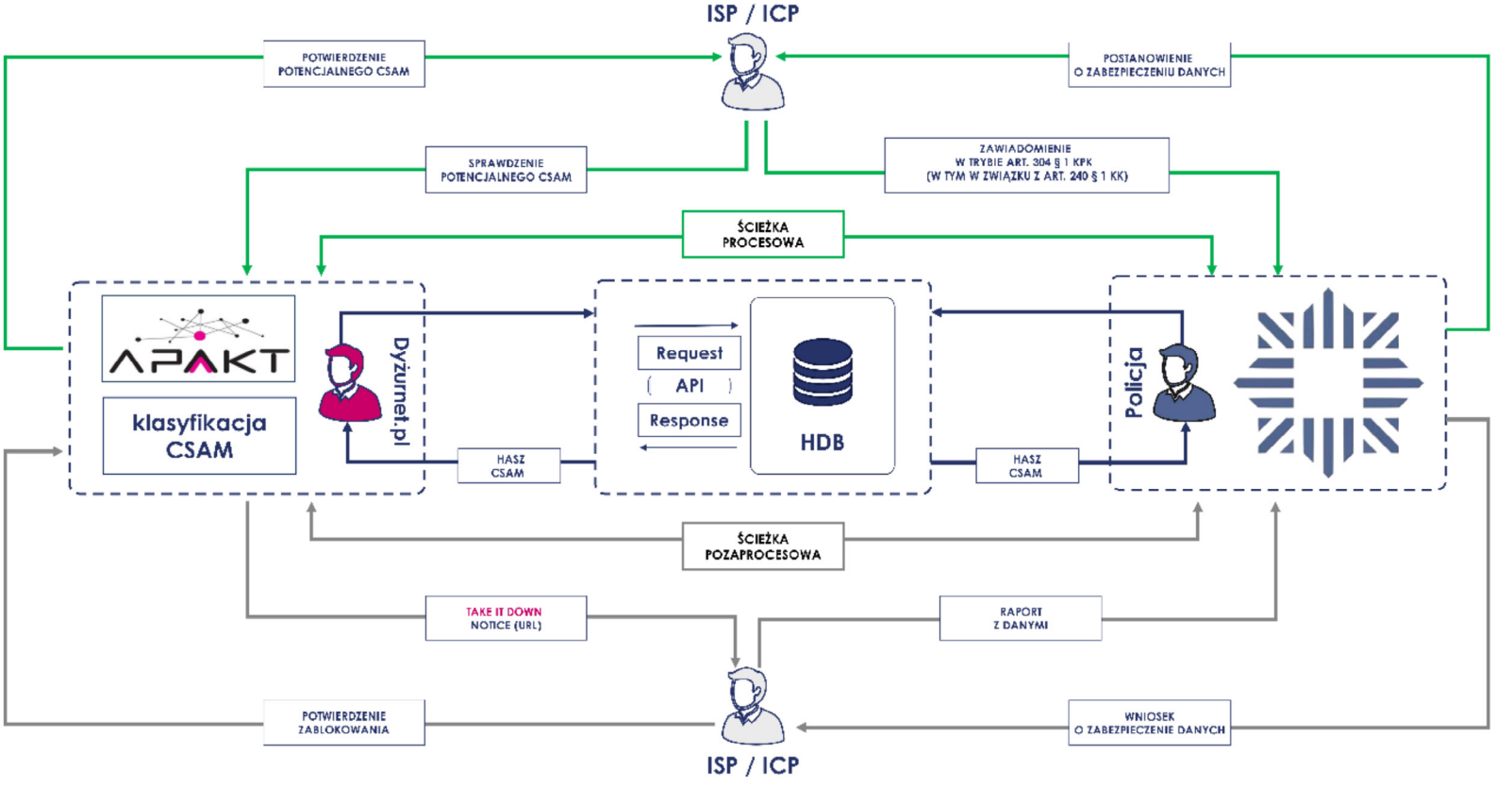
Widoczne opóźnienia mogą dziwić, zwłaszcza w kontekście powszechnej akceptacji wykorzystywania różnego rodzaju międzynarodowych baz danych, „w których gromadzone są informacje dotyczące np. terroryzmu, przestępczości narkotykowej, handlu ludźmi i bronią, kradzieży dzieł sztuki, dziecięcej pornografii oraz innych form przestępczości zorganizowanej" (Moszczyński, 2020, s. 710). Tenże sam autor, odnosząc się do ogólnych korzyści wynikających z posiadania dostępu do baz, konstatuje:

> Skomputeryzowane bazy danych oraz różnego rodzaju zbiory, registratury i kartoteki odgrywają w kryminalistyce bardzo ważną rolę w procesie zwalczania przestępczości. Wykorzystywane są do typowania i wykrywania sprawców przestępstw, kojarzenia i analiz różnego rodzaju zdarzeń, ustalania tożsamości osób (...), prowadzenia badań kryminalistycznych, koordynacji działań Policji i innych służb, wymiany informacji, prognozowania rozwoju przestępczości, przeprowadzania analiz statystycznych i innych celów (s. 703).

Poniżej przedstawiono wizualizację koncepcji jednego z podsystemów, tj. bazy haszy (rys. 10), który mógłby realizować wszystkie wyżej wymienione funkcje i zadania właśnie w odniesieniu do walki z CSAEM. Koncepcja zakłada istnienie centralnej, zautomatyzowanej bazy haszy (tu: ang. *hash datbase*, HDB), do której bezpośredni dostęp mają wskazane w *Krajowym Planie* podmioty – Policja oraz Dyżurnet.pl NASK PIB. Nie mniej ważnym elementem są tu IES/ESP, które w ramach całego procesu stanowią stronę aktywną w zakresie blokowania dostępu do treści CSAEM, zabezpieczania danych na potrzeby postępowań karnych (i innych), a także podmiotu zawiadamiającego. W związku z dynamicznymi zmianami w legislacji krajowej i unijnej w niedalekiej przyszłości to oni – na polecenie uprawnionych organów ścigania i wymiaru sprawiedliwości – mogą być odpowiedzialni również za usuwanie ww. danych.

Rys. 10.

Koncepcja krajowej bazy CSAM – podsystem haszy (opracowanie własne)

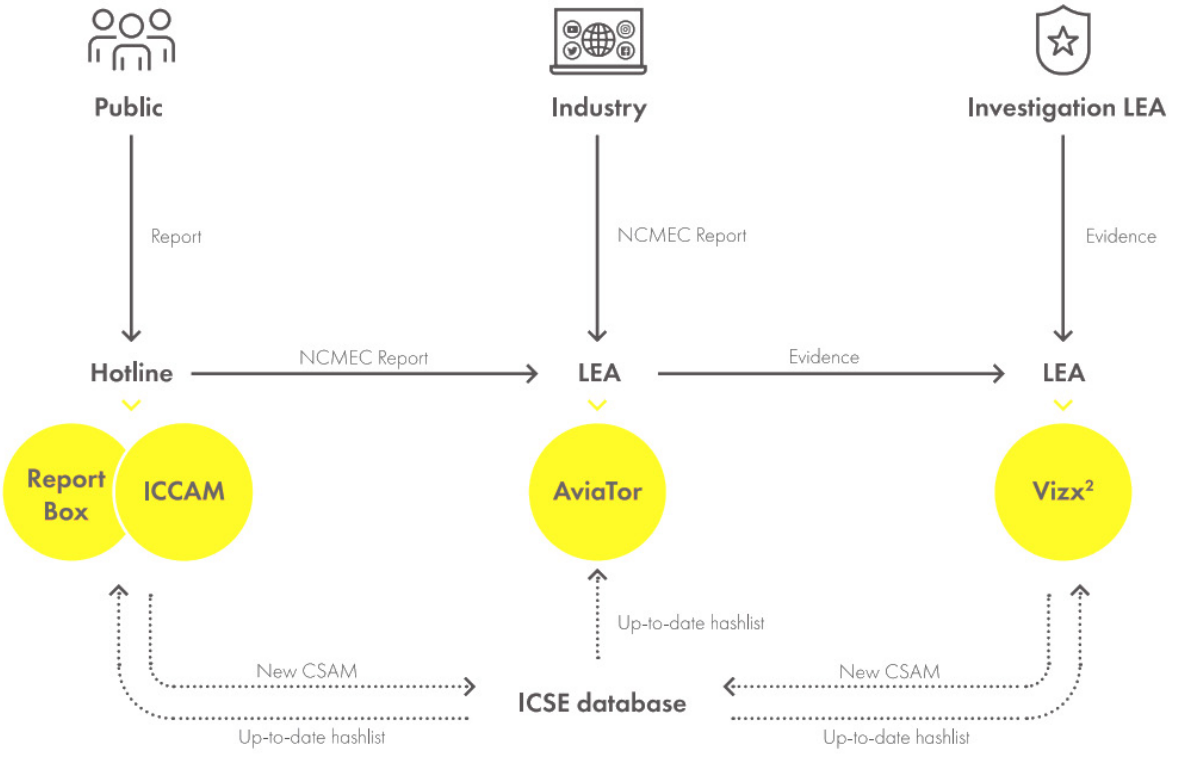


Zanim przejdziemy do omówienia poszczególnych rozwiązań, za pośrednictwem których funkcjonariusze lub specjaliści wskazanych podmiotów będą mogli przetwarzać, analizować i klasyfikować treści CSAEM, warto pochylić się nad jedną z koncepcji takiego systemu (wysokopoziomowe, międzysektorowe rozwiązanie problemu walki z CSAEM), którą zaproponował ZIUZ, realizujący m.in. projekt AVIATOR.

Przywołany przykład zawiera wszelkie wspomniane wcześniej elementy, w tym kierowane do organów ścigania oprogramowanie do klasyfikacji treści (VizX2), obsługę raportów NCMEC (AVIATOR) oraz raportowanie do krajowego punktu zgłoszeń (*hotline*) przez obywateli. Zdaniem Autora podczas tworzenia krajowego, zcentralizowanego systemu teleinformatycznego (bazy CSAM) – aspirującego do bycia skutecznym, wydajnym, a przede wszystkim wieloletnim rozwiązaniem – należy wziąć pod uwagę istniejące już modele zagraniczne (np. szwedzki, brytyjski, francuski czy rumuński), o funkcjonalnościach analogicznych do poniższego (rys. 11), a następnie, w drodze szczegółowej analizy potrzeb krajowych, dokonać ich ewaluacji w celu stworzenia najlepszego dla Polski narzędzia.

Rys. 11.

System wymiany haszy plików zawierających treści CSAEM (opracowanie: ZIUZ)



Przykład 1. ZIUZ VizX2/Fenzoz

Platforma VizX2 Forensic (ZIUZ, 2023a) oraz program Fenzoz (ZIUZ, 2023a) są przeznaczone do informatyki śledczej zorientowanej na CSAEM (przetwarzanie, analiza i klasyfikacja zdjęć i wideo). Rozwiązanie to umożliwia przeszukiwanie w uporządkowany sposób znacznych ilości treści audiowizualnych, zapewniając jednocześnie użytkownikowi szybki wgląd w całość sprawy. Według informacji dostępnych na 2025 r. producent oferował wersję do użytku zarówno na pojedynczym stanowisku, jak i do pracy zespołowej – Teamwork (1–20 osób) lub Datacenter (20–100+).

Program posiada takie funkcje, jak: przeglądanie treści wizualnych w różnych formatach, *carving*, wyszukiwanie i filtrowanie, np. na podstawie haszy czy danych *exif*. Najważniejszym elementem jest jednak środowisko do klasyfikacji, zapewniające także detekcję twarzy oraz prekategoryzację nowych treści – dzięki modułowi Cortado AI (ZIUZ, 2023c), a także *cross-checking* z interpolową bazą haszy ICSEdb – dzięki modułowi ICARE.

Przykład 2. Griffeye (Advanced)

Griffeye[7] to rozwiązanie szwedzkiej firmy Griffeye Technologies AB (pod koniec 2023 r. wykupione przez Magnet Forensics), dobrze znane wśród zagranicznych organów ścigania (i coraz częściej stosowane też w Polsce). Według danych producenta korzysta z niego ponad 4000 różnych agencji/organów ścigania w ponad 80 krajach). Jest to rozwiązanie wykorzystywane m.in. zarówno przez europolowe AP TWINS, jak i interpolowe ICSE. Model licencjonowania obejmuje pojedynczego użytkownika/stanowiska (Advanced), organizację lokalną (Operations), a także organizację szczebla krajowego (Enterprise).

Opis działania

1. Pozyskiwanie potencjalnego *CSAEM*. Program pozwala na załadowanie, w celu dalszego przeprocesowania (wstępny etap przetwarzania), kopii kryminalistycznych w większości formatów (np. 001, AFF, E01, BIN, DD, DMG, E01, EWF, VHD, VMDK) czy plików JSON (na potrzeby VIC Case), a także folderów z przygotowaną uprzednio zawartością (np. zdjęcia, wideo). Na tym etapie można również skonfigurować opcje wykrycia i odzysku danych usuniętych, utraconych czy nadpisanych. W dalszej kolejności wskazuje się typ danych, które mają zostać przetworzone (obrazy, wideo, dokumenty, archiwa), przy czym można skorzystać z opcji wykrywania niezgodności między formatem a rozszerzeniem (m.in. X-ways Foreniscs również posiada tę funkcję). Funkcja

7 Na potrzeby artykułu testowano Griffeye Advanced w najnowszej wersji 25.5.0 (grudzień 2025 r.).

ta pozwala ujawnić pliki zawierające zapis wizualny (np. zdjęcie w formacie JPEG), ale rozszerzenie typowe dla dokumentu (np. znany z pakietu MS Office .doc czy .docx).

W dalszej kolejności można zdefiniować sposoby przeprocesowania materiałów. Znajduje się tu m.in. sekcja odpowiadająca za konfigurację GID (ang. *Griffeye Intelligence Database*) – wbudowanego rozwiązania, które umożliwia agregowanie, importowanie, uzupełnianie i eksportowanie informacji mogących wspomóc i przyspieszyć proces kategoryzacji CSAEM. Mogą to być przykładowo: dane grupujące (kategorie, serie, tagi), dane o statusie materiałów wizualnych (znane/nieznane/dystrybuowane w sieci Internet) czy o statusie osób widocznych na obrazie (zidentyfikowany pokrzywdzony/sprawca).

Na tym etapie wybiera się sposób przetworzenia zdjęć i wideo, np. wyliczenie wartości hasz algorytmem PhotoDNA, wykrycie podobieństw i nagości, grupowanie (ang. *stack*), dziedziczenie przez kopie wizualne informacji przyporządkowanych do „rodzica" (tj. zdjęcia, w stosunku do którego wyliczane jest procentowe podobieństwo innych treści), a także sposoby prezentacji materiałów wideo (kolaż oraz pobranie przetwarzanych następnie klatek).

Przedostatnim krokiem, mającym na celu przyspieszenie analizy, jest utworzenie filtrów wykluczających dane z dalszego przetwarzania (np. materiałów wideo, kiedy wiadomo, że należy skupić się tylko na zdjęciach). Ten wstępny etap kończy uzupełnienie tzw. metryczki, która będzie opisywać sprawę – mogą to być np. dane analityka/biegłego, dane związane ze sprawcą, liczba porządkowa (lp.) dochodzenia/śledztwa czy sygnatura sprawy według notacji prokuratury czy sądu.

2. Selekcja. Zaletą programu Griffeye jest optymalizacja selekcji i analizy materiałów audiowizualnych, a także dobrze zaprojektowany interfejs użytkownika, pozwalający – w ramach tzw. przestrzeni roboczych (ang. *workspace*) – w sposób intuicyjny i szybki (co szczególnie ważne przy liczbie plików CSAEM powyżej kilku tysięcy) organizować, przeglądać i wyszukiwać dane.

Zaimplementowane sposoby grupowania, filtrowania i prezentowania CSAEM oraz metadanych są proste i łatwo konfigurowalne. Selekcja odbywa się głównie w oparciu o kategoryzację (istnieją predefiniowane kategorie i integracja z GID) oraz klasyfikację (można ją budować m.in. w oparciu o *bookmarks*, *tags*), a także bardzo rozbudowane filtry, w tym różnego rodzaju metadane dotyczące: systemowych właściwości plików (np. format, typ, wielkość w bajtach, rozmiar w pikselach, znaczniki czasu), danych *exif* (np. informacje geolokalizacyjne, numer seryjny, autor), czy też metadane będące artefaktami przetwarzania zapisów wizualnych za pomocą oprogramowania (np. nazwa i wersja programu, czy od niedawna prompt, oraz informacja o wykorzystanym modelu AI).

W obrębie przestrzeni roboczej dostępnych jest kilka metod przeglądania materiałów. Nawigacja pomiędzy nimi może w sposób znaczący przyspieszyć wyszukiwanie oraz selekcję (oznaczanie: kategorią, markerem lub tagiem). Widok w trybie „Thumbnail" pozwala na równoczesny podgląd zdefiniowanej liczby miniaturek reprezentujących obraz. Widok w trybie „Grid" pozwala na podgląd w formie tabeli (siatki). Jest to widok bardzo zbliżony do interfejsu programu X-ways Forensics, posiadający filtry zakładane na poszczególne kolumny (opisane nagłówkami wskazującymi nazwą na zawartość, np. kategoria, wartość hasz SHA-1, poziom nagości itd.). Trzecim głównym trybem podglądu jest „Search" (wyszukiwanie), w którym można dokonać selekcji zdjęć przy użyciu zdjęcia referencyjnego, np. z wizerunkiem sprawcy lub relewantnego dla sprawy miejsca.

Jak już wspominano, Griffeye jest intuicyjny i zoptymalizowany do pracy z materiałami wizualnymi, co przejawia się m.in. w podziale przestrzeni roboczej na opisane tu tryby podglądu, klarowne rozmieszczenie na kilku paskach (podzielonych dodatkowo na opisane sekcje) narzędzi wspomagających analizę czy też dużej liczbie skrótów klawiszowych, które – po ich opanowaniu – znacznie przyspieszają wykonanie poszczególnych czynności.

Oferowane przez program sposoby manualnej lub (semi)zautomatyzowanej selekcji danych wzbogacono o możliwość automatycznego grupowania i filtrowania w oparciu o *Griffeye Intelligence Database* (GID). Dzięki GID możliwe jest przetworzenie treści wizualnych w oparciu o dostępne, zaufane źródła, np. bazy VIC Project czy ICSE. Bez rozwijania zagadnienia, na które można by poświęcić odrębny artykuł, warto wspomnieć, że obie przykładowe bazy posługują się kilkupoziomowym opisem obrazów, a nie tylko np. wartością hasz.

Skuteczność implementacji rozwiązania opartego na bazie haszy nie leży w uzyskaniu zerojedynkowego potwierdzenia: „znaleziono dopasowanie"/„nie znaleziono dopasowania". Rzeczywisty potencjał takiej bazy – automatyzującej przetwarzanie wielomilionowych zbiorów obrazów – ujawnia się dopiero na etapie synchronizacji wszystkich dostępnych informacji, np.: brak dopasowania wartości MD5 – zgodność na poziomie PhotoDNA – zidentyfikowany pokrzywdzony – materiały dystrybuowane w sieci – metadane (np. znacznik geolokalizacji wskazujący konkretne miasto w Polsce).

Takie usystematyzowanie i skorelowanie heterogenicznych danych (por. rys. 6) pozwala na skuteczną analizę, a tym samym wydobycie z materiału dowodowego wszystkich informacji, które mogą być istotne dla rozstrzygnięcia sprawy, w tym również na potrzeby identyfikacji osób pokrzywdzonych (VID).

Program oferuje również preklasyfikację treści w oparciu o kilka modeli AI, w tym znany od lat, natywnie wbudowany moduł BRAIN oraz model Thorna, uznawany za jeden z lepszych modeli detekcyjnych na świecie.

Omówione powyżej etapy postępowania z treściami CSAEM dotyczą jednego użytkownika/stanowiska. Potencjał narzędzia, a przede wszystkim ludzi (od pracy operacyjnej, przez wstępny etap przetwarzania realizowany przez informatyka śledczego, aż po rozbudowaną analizę, kategoryzację i klasyfikację treści na potrzeby procesu karnego), może zostać w pełni wykorzystany dopiero poprzez wprowadzenie rozwiązań integrujących pracę zespołów na poziomie regionalnym (Griffeye Operations) lub krajowym (Griffeye Enterprise).

Warto nadmienić, że podobne rozwiązania oferowane są przez firmę Semantics 21 (por. https://www.semantics21.com/s21-visionx/) oraz BlueBear (por. https://bb-les.ca/). Zasadniczą różnicą pomiędzy tymi produktami jest ich przeznaczenie, tzn. VisionX – pierwszego z ww. producentów – funkcjonalnie jest bardzo zbliżony do Griffeye'a. Oferuje kilka modeli AI: moduł do prekategoryzacji, moduł do detekcji AIG CSAEM, moduł deskrypcji w języku angielskim zapisów wizualnych (zdjęć) oraz predykcji geolokalizacji. Posiada także możliwość integracji z bazą haszy, Project Arachnid oraz NCMEC. BlueBear opisuje swoje narzędzie, tj. LACE, jako stworzone do szybkiej kategoryzacji dużych ilości plików na potrzeby procesu karnego. Griffeye ma być natomiast rozwiązaniem do CSAEM i OCSAE o szerokim zastosowaniu, a VisionX – narzędziem służącym przede wszystkim do identyfikacji pokrzywdzonych.

Wracając do zastosowań wielkoskalowych. Sprawa (ang. *case*), a przede wszystkim pozyskana w toku czynności operacyjno-rozpoznawczych czy dochodzeniowo-śledczych wiedza, nie musi się kończyć w papierowych aktach przechowywanych w archiwach. Dedykowany zespół regionalny (zarząd, właściwa komórka wojewódzka, itp.), realizując postępowanie o zasięgu krajowym czy międzynarodowym, może zasilić haszami sklasyfikowanych/skategoryzowanych plików cały system. Zwiększą w ten sposób szybkość prowadzenia kolejnych spraw, a ponadto – przy kolejnej realizacji – zmniejszą ekspozycję swoją lub innego zespołu na treści CSAEM. Co jeszcze bardziej istotne, delegowanie czynności na zautomatyzowane narzędzia do informatyki śledczej zwiększa prawdopodobieństwo realizacji priorytetowych zadań z zakresu VID czy PID.

Platformy do gromadzenia, przetwarzania i wymiany informacji o CSAEM i OCSAE

Przykład 1. ICCAM i CPORT

W przedstawionym powyżej modelu ZIUZ oraz w wymienionych narzędziach wykorzystywanych w informatyce śledczej uwzględniono współpracę międzysektorową pomiędzy organami ścigania oraz punktem zgłoszeń (ang. *hotline*). W Polsce funkcję krajowego *hotline'u* od blisko 25 lat pełni Dział Reagowania na Nielegalne Treści w Internecie Dyżurnet.pl, który jest częścią CSIRT NASK, a także organizacji

INHOPE, zrzeszającej niemal 60 *hotline'ów* na całym świecie. Dyżurnet.pl funkcjonuje w oparciu o ustawę o krajowym systemie cyberbezpieczeństwa. Dostępny jest – przez mObywatela i formularz na stronie https://dyzurnet.pl – dla każdej osoby zainteresowanej zgłoszeniem nielegalnych czy szkodliwych treści zagrażających dzieciom. Razem z Fundacją Dajemy Dzieciom Siłę stanowi część programu Safer Internet.

Dyżurnet.pl realizuje m.in. zadania wspomnianego powyżej *Krajowego Planu Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich na lata 2023–2026*, bierze też udział w opracowaniu i wdrażaniu *The Universal Classification Schema* (międzynarodowego standardu klasyfikacji treści CSAEM). Ponadto inicjuje i współtworzy: badania, kampanie, projekty, technologie, publikacje, materiały edukacyjne, zmiany legislacyjne.

Dyżurnet.pl działa w przestrzeni międzynarodowej (m.in. współpracując z punktami zgłoszeń z innych krajów) i międzysektorowej (zarówno z organami ścigania, jak i ISP/ICP). Taki model współpracy umożliwia wykorzystanie wiedzy zdobytej przez całą organizację (INHOPE) (por. raporty INHOPE oraz Dyżurnet.pl). Jako *hotline* zrzeszony w INHOPE, wykorzystuje platformę ICCAM.

> W 2015 r. INHOPE, we współpracy z Komisją Europejską, uruchomił system ICCAM (*I-'See'(C)-Child-Abuse-Material*), który jest przede wszystkim platformą umożliwiającą szybką wymianę informacji o materiałach CSAM pomiędzy *hotline'ami* z różnych krajów. (…) ICCAM to bezpieczne oprogramowanie INHOPE, które przetwarza adresy URL, neutralne obrazy oraz nagrania wideo, łącząc się z centralną infrastrukturą teleinformatyczną Interpolu, a następnie klasyfikuje te materiały (…). Po potwierdzeniu CSAM tworzony jest odpowiedni raport, który następnie trafia do właściwego krajowego *hotline'u* zrzeszonego w INHOPE (Kumar i in., 2022).

ICCAM unifikuje i optymalizuje pracę specjalistów z zakresu analizy i klasyfikacji treści CSAEM na całym świecie. Obecnie INHOPE modernizuje system klasyfikacji treści, dopasowując go do *The Universal Classification Schema*, co umożliwi wzbogacenie stosunkowo prostej informacji krajowej (kategoria: legalny – nielegalny) o dodatkowe elementy, jakie można wykorzystać do skuteczniejszego blokowania i usuwania treści przedstawiających seksualne wykorzystywanie dzieci z przestrzeni internetu, a także pełniejszego zrozumienia zjawiska i jego globalnych przemian, o których była mowa w pierwszej części tego artykułu.

ICCAM jest narzędziem teleinformatycznym zintegrowanym z interpolową bazą ICSE. Analitycy działający w ramach INHOPE stanowią dodatkowy element budowania skutecznej odpowiedzi na CSAEM i OCSAE jako form międzynarodowej

przestępczości zorganizowanej. Dzieje się tak dlatego, że zgodnie z procedurami regulującymi działalność *hotline'ów* mają one obowiązek zgłaszać właściwym krajowym organom ścigania fakt ujawnienia potencjalnie nielegalnych treści. Tym samym współpraca międzynarodowa w ramach INHOPE wpływa na cyberbezpieczeństwo krajowe. Sklasyfikowane przez *hotline* treści CSAEM mogą zasilać również krajowe bazy kryminalistyczne.

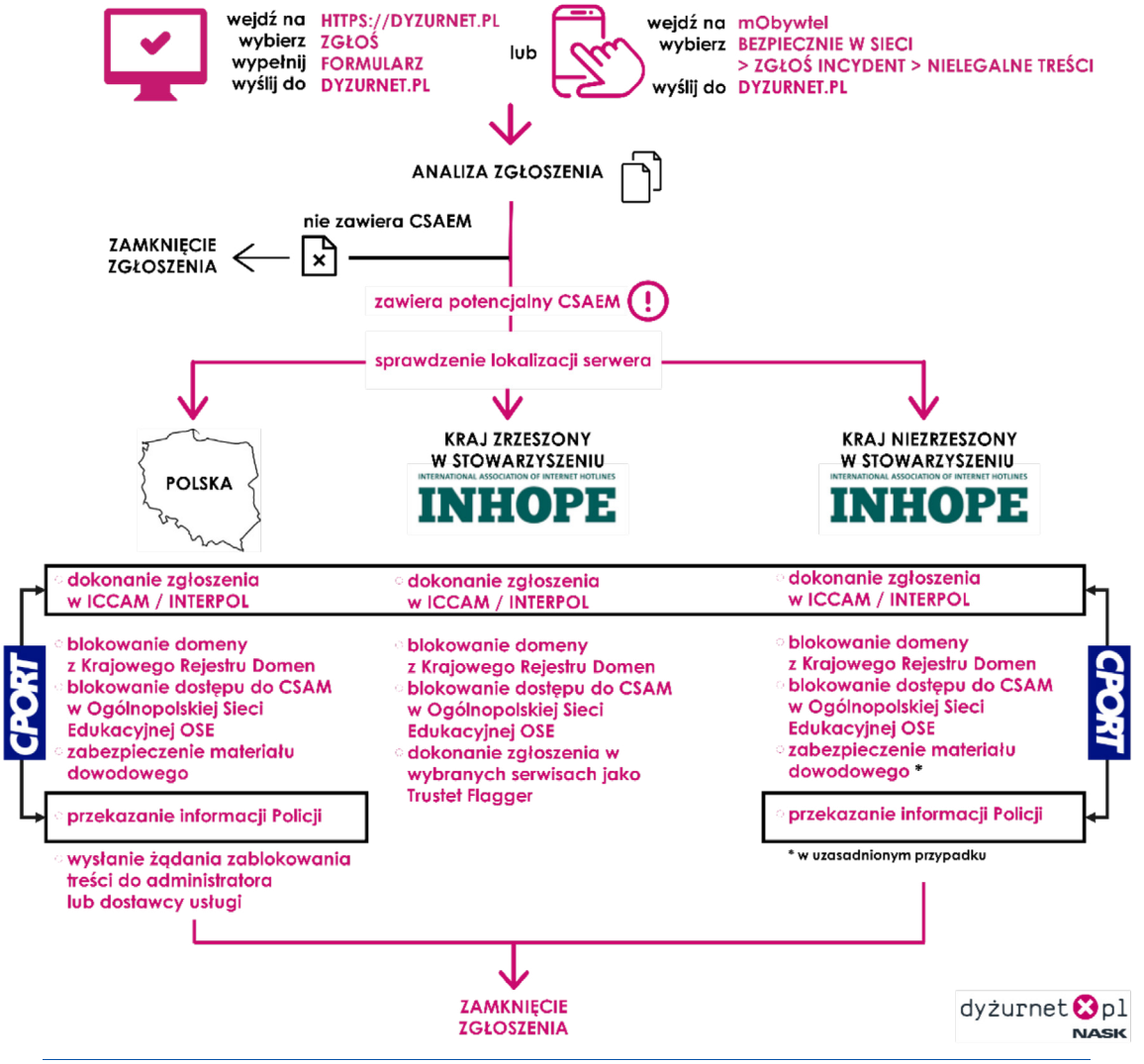
> Na poziomie krajowym kilka agencji prowadzi własne repozytoria materiałów przedstawiających wykorzystywanie seksualne dzieci, a część z nich jest połączona z bazą danych ICSE (ECPAT, 2018). Wśród nich warto wymienić: *National Child Victim Identification System* (NCVIS) w Stanach Zjednoczonych, *Child Abuse Images Database* w Wielkiej Brytanii (CAID) oraz *National Centre for the Analysis of Child Pornography Images* we Francji (CNAIP/CALIOPE).
>
> Policja może również korzystać z narzędzi analitycznych (ang. *intelligence tools*), które usprawniają wymianę informacji między federalnymi, stanowymi i lokalnymi organami ścigania, np. *Child Exploitation Tracking System* (CETS) – oprogramowanie opracowane przez Microsoft we współpracy z kanadyjskimi organami ścigania, obecnie używane (lub planowane do wdrożenia) w różnych krajach. (...) Systemy służące do rozpoznawania obrazów i wymiany informacji mają również na celu ograniczenie powielania pracy, umożliwiając śledczym sprawdzenie, czy dany obraz został już odkryty w innym kraju lub jurysdykcji oraz czy podejrzany został już zidentyfikowany w innych postępowaniach lub są wobec niego obecnie prowadzone czynności (Macilotti, 2022, s. 231).

Dyżurnet.pl przesyłał do wskazanej komórki organizacyjnej Policji specjalnie w tym celu opracowany raport, który może stanowić podstawę do podjęcia dalszych czynności. W związku z rosnącą liczbą zgłoszeń i plików, aby uniknąć opóźnień (ang. *backlog*) już na etapie przekazywania informacji, planuje się wdrożenie w Polsce skierowanego do Policji systemu o nazwie CPORT.

CPORT jest wdrażanym na świecie rozwiązaniem teleinformatycznym automatyzującym i przyspieszającym znaczną część czynności związanych z wymianą informacji pomiędzy krajowym punktem zgłoszeń (*hotline*) a jednostką Policji wyznaczoną do walki z CSAEM i OCSAE. Platforma CPORT – opracowana przez INHOPE we współpracy z Interpolem – służy do przekazywania w czasie rzeczywistym (minuty zamiast dni) uprawnionym funkcjonariuszom Policji informacji i danych na poziomie krajowym o treściach przedstawiających seksualne wykorzystywanie dzieci. W odniesieniu do wymiany informacji CPORT zapewnia: bezpieczeństwo (bez potrzeby przewożenia, archiwizacji czy utylizacji nośników danych), legalność (trójstronne

porozumienie gwarantujące działanie zgodne z prawem krajowym i międzynarodowym), dostęp bezpośredni (bez opóźnień wynikających z obiegu kancelaryjnego pism i nośników), kompletność informacji (dane wystarczające do podjęcia pierwszych czynności), agregację (możliwość powrotu do spraw zamkniętych/zamrożonych) oraz specjalistyczną wiedzę (m.in. wgląd w klasyfikację i kategoryzację treści wykonaną przez specjalistów Dyżurnet.pl). Po wdrożeniu obieg danych i informacji pomiędzy Dyżurnet.pl i Policją mógłby wyglądać w sposób przedstawiony poniżej (rys. 12).

Rys. 12.
Integracja systemu zgłoszeń Dyżurnet.pl i Policji w oparciu o CPORT (opracowanie: Dyżyrnet.pl)



Przykład 2. Project Arachnid i Arthropod

Kolejnym elementem systemu zwalczania CSAEM i OCSAE są wielozadaniowe rozwiązania teleinformatyczne, integrujące działania reaktywne (m.in. reagowanie na zgłoszenia, utrzymywanie i rozwój baz CSAM, kategoryzacja / klasyfikacja treści) oraz proaktywne (m.in. *crawlery* i *scrapery*).

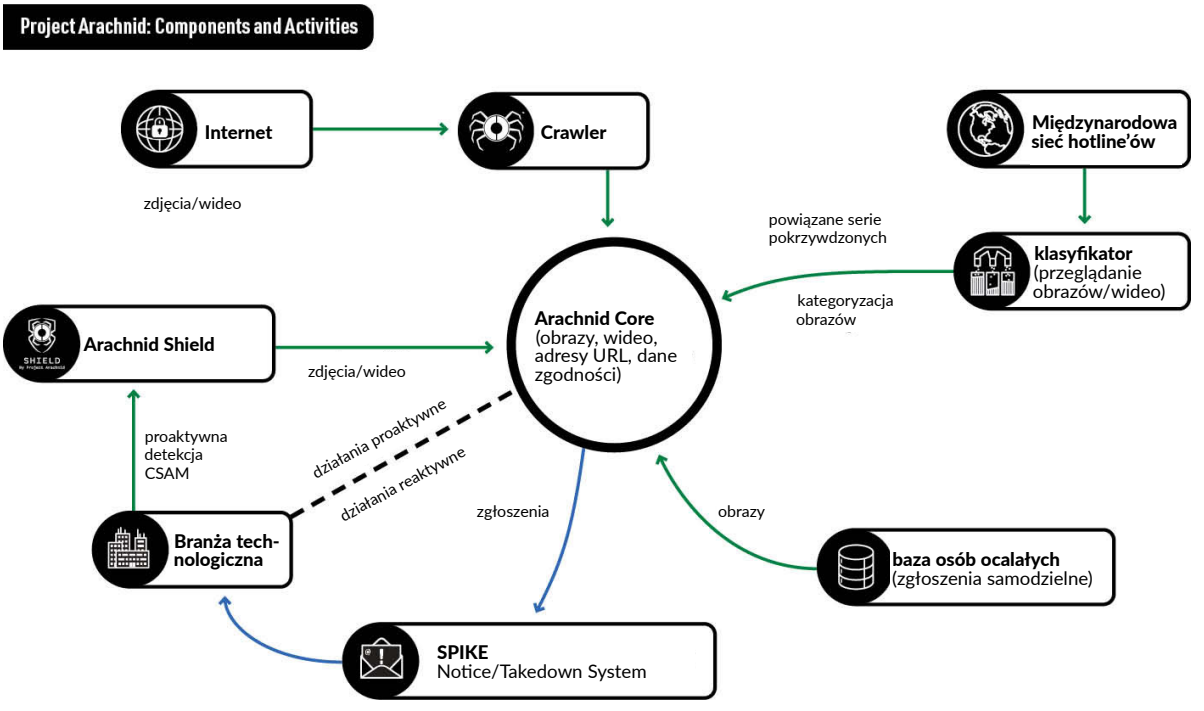
Za przykład niech posłuży Project Arachnid (C3P, 2023, 2026) – kanadyjska inicjatywa o zasięgu międzynarodowym, zrzeszająca 18 światowych podmiotów zaangażowanych w walkę z CSAEM i OCSAE, w tym ponad 50 analityków z 17 krajów. Do zadań Arachnid od blisko 10 lat należy m.in. automatyczne skanowanie internetu (stały monitoring miejsc zagrożonych), wyszukiwanie materiałów przedstawiających seksualne wykorzystywanie dzieci oraz zgłaszanie ich do zablokowania lub usunięcia i dalszej analizy przez ekspertów. Według danych pochodzących ze strony projektu, platforma przetworzyła ponad 176 mld zdjęć, a ponad 126 mln potencjalnie nielegalnych treści przekazała do dalszej analizy, co skutkowało ponad 141 mln tzw. *takedown notices*, tj. oficjalnych zgłoszeń z żądaniem natychmiastowego usunięcia treści skierowanych m.in. do administratorów stron, hostingów, platform (stan na początek 2026).

Omawiane rozwiązanie warte jest zwrócenia uwagi z kilku względów. Po pierwsze, działa proaktywnie, co oznacza, że dane są wyszukiwane w czasie rzeczywistym przez *crawler* (automatyczne narzędzie służące do indeksowania zasobów sieciowych), a następnie – w uzasadnionym przypadku (tj. podejrzenie obecności treści CSAEM) – pobierane przez *scraper*. Po drugie, system pozwala na korzystanie z wydzielonych wskazanym odbiorcom zasobów poprzez odseparowane moduły, takie jak Arthropod (dla Policji) czy Shield (dla podmiotów komercyjnych). Po trzecie – wykorzystuje opisaną już tu technologię haszy w możliwie najszerszym zakresie:

> Arachnid to zautomatyzowany *crawler* internetowy o zasięgu międzynarodowym, który wykrywa i przetwarza dziesiątki tysięcy obrazów na sekundę oraz wysyła powiadomienia o konieczności usunięcia treści do dostawców usług online (…). [W tym celu] wykorzystuje technologię haszowania, aby dopasowywać konkretne zdjęcie lub nagranie wideo do bazy znanych materiałów CSEA. Technologia haszowania może być dokładna (gdy jeden obraz jest identyczny z drugim) albo może wskazywać dopasowanie przybliżone, np. w przypadku zmienionego rozmiaru obrazu. Dopasowania przybliżone uzyskuje się dzięki „haszom percepcyjnym" lub oprogramowaniu Microsoft PhotoDNA. Arachnid udostępnia firmom API, przez które moderatorzy treści lub dostawcy hostingu mogą proaktywnie porównywać nowo przesyłane lub istniejące już materiały z listą cyfrowych odcisków (ang. *digital fingerprints*) przygotowaną przez Arachnid (OECD, 2023, s. 26).

Działania proaktywne przy użyciu *crawlerów* czy w ramach tzw. *proactive investigations* (Francis i in. 2021) pozwalają bądź przerwać dystrybucję CSAEM, bądź też gromadzić niezbędny do skazania sprawców dalszy materiał dowodowy. Model działania takiego narzędzia przedstawiono poniżej (rys. 13).

Rys. 13.
Projekt Arachnid – model działania (opracowanie: https://projectarachnid.ca/)



Jednostki specjalne do walki z CSAEM i OCSAE

Kolejnym z elementów krajowego systemu – obok omówionych powyżej technologii – powinna być odpowiednio przygotowana agencja/jednostka Policji, która byłaby w stanie dynamicznie dokonywać oceny swojej skuteczności, w razie potrzeby modyfikować struktury lub sposób organizacji, a także rozwijać nowe metody i narzędzia.

We wspomnianym badaniu uczestnicy zwrócili uwagę na to, że: „praca w wyspecjalizowanych jednostkach policji zajmujących się przestępstwami na tle seksualnym, zwiększa skuteczność czynności z zakresu zwalczania CSEA" (Tselenti, 2025, s. 7).

Podobnego zdania są eksperci z Interpolu, którzy od lat podnoszą kwestię konieczności tworzenia specjalistycznych struktur krajowych:

> Tam, gdzie jeszcze nie istnieją, należy utworzyć i odpowiednio wyposażyć krajowe wyspecjalizowane jednostki dedykowane do zwalczania OCSEA (ang. *national specialized units dedicated to combatting* OCSEA). W tym zakresie międzynarodowa sieć specjalistów Interpolu ds. przestępstw przeciwko dzieciom jest gotowa wspierać rozwój kompetencji w tej dziedzinie. Po podłączeniu do bazy ICSE jednostki te uzyskają możliwość analizowania materiałów przedstawiających seksualne wykorzystywanie dzieci, identyfikacji pokrzywdzonych oraz sprawców zarówno na poziomie krajowym, jak i w ramach wspólnych operacji międzynarodowych (Interpol, 2022b, s. 11).

Dlatego też na rozwój ICAC (ang. *Interpol's Crimes Against Children Unit*) przeznaczono 11 mln euro, które mają zostać wykorzystane na modernizację funkcjonującej bazy CSAM, w efekcie czego obecnie powstaje ICSE NG (ang. *next generation*).

Szukając kryteriów, którymi mogłyby cechować się takie specjalistyczne jednostki, można posłużyć się modelem przedstawionych w ramach OOSI (ang. *Out Of The Shadows Index*). Według cytowanego źródła skuteczny, krajowy, międzysektorowy system ochrony dzieci musi posiadać strukturę policyjną, która uzyskała wskaźnik „potencjału" najbliższy 100. Ważnym elementem przedstawionego modelu jest wyróżnienie wśród jednostek/agencji dwóch poziomów, tj. komórek wyspecjalizowanych (ang. *dedicated unit*), dla których zwalczanie CSAE i OCSAE stanowi priorytet i mieści się w ich podstawowych kompetencjach, oraz jednostek wyznaczonych (ang. *designated unit*). W przypadku tych drugich jednostka nie musi koncentrować się wyłącznie na (internetowych) przestępstwach seksualnych wobec dzieci, jednak problematyka ta stanowi wyraźną część zakresu jej działania. Poniżej przedstawiono kryteria podlegające ocenie:

Potencjał Policji (ang. *Police Capacity*) – ogólna ocena przygotowania instytucjonalnego oraz operacyjnego formacji (od 0 do 100):

1. Wyspecjalizowana jednostka (ang. *dedicated unit*) ds. wykorzystywania seksualnego dzieci – istnienie odrębnej jednostki zajmującej się wyłącznie przestępstwami seksualnymi wobec dzieci.
2. Wyspecjalizowana jednostka (ang. *dedicated unit*) ds. internetowych przestępstw seksualnych wobec dzieci – funkcjonowanie specjalistycznego zespołu zwalczającego wykorzystywanie dzieci w cyberprzestrzeni.
3. Wyznaczona jednostka (ang. *designated unit*) ds. internetowego CSAE – formalne wskazanie komórki odpowiedzialnej za prowadzenie spraw dotyczących wykorzystywania dzieci *online*.

4. Wyznaczona jednostka (ang. *designated unit*) ds. informatyki śledczej w zakresie internetowego CSAE – dostępność zaplecza technicznego i eksperckiego do analizy materiałów cyfrowych związanych z przestępstwami seksualnymi na szkodę dzieci.
5. Wyznaczona jednostka (ang. *designated unit*) do realizacji międzynarodowych spraw z zakresu internetowego CSAE – zdolność do prowadzenia spraw transgranicznych i współpracy z zagranicznymi organami ścigania.
6. Szkolenia z prowadzenia postępowań w postaci przyjaznej dzieciom (ang. *training on child-friendly investigations*) – przygotowanie funkcjonariuszy do prowadzenia czynności z udziałem dziecka w sposób zapewniający jego bezpieczeństwo psychiczne, poszanowanie godności oraz ograniczenie ryzyka wtórnej wiktymizacji w sprawach CSAEM i OCSAE.
7. Narzędzia i standardy postępowania funkcjonariuszy przyjazne dzieciom, a także młodzieży (ang. *child and adolescent-friendly tools and standards for investigators*) – stosowanie procedur i wytycznych dostosowanych do wieku i potrzeb dzieci oraz nastolatków (patrz pkt 6).
8. Przyjazne dzieciom oraz młodzieży standardy przesłuchania (ang. *child and adolescent-friendly tools and standards for interviewing*) – wykorzystywanie specjalnych metod rozmowy z dziećmi, takich jak jedno przesłuchanie czy wsparcie psychologa.
9. Liczba funkcjonariuszy policji na 100 000 mieszkańców (ang. *Police personnel per 100 000 persons*) – wskaźnik ogólnej dostępności zasobów kadrowych policji, wpływający na skuteczność reagowania także w sprawach dotyczących dzieci.

Według powyższego Indeksu tak przedstawiała się gotowość dwóch wybranych państw europejskich w 2022 r.:

Tabela 4.

Wyniki analizy przeprowadzonej według modelu OOSI w odniesieniu do Wielkiej Brytanii oraz Albanii (opracowanie: https://outoftheshadows.global/data/europe-and-central-asia/)

	wskaźniki	Wielka Brytania	Albania
	Potencjał Policji (ang. Police capacity)	90,9	85,1
1.1	Wyspecjalizowana jednostka (ang. dedicated unit) ds. wykorzystywania seksualnego dzieci	100	100
1.2	Wyspecjalizowana jednostka (ang. dedicated unit) ds. internetowych przestępstw seksualnych wobec dzieci	100	66,7
1.2.1	Wyznaczona jednostka (ang. designated unit) ds. internetowego CSAE	100	100
1.2.2	Wyznaczona jednostka (ang. designated unit) ds. informatyki śledczej w zakresie internetowego CSAE	100	0
1.2.3	Wyznaczona jednostka (ang. designated unit) do realizacji międzynarodowych spraw z zakresu internetowego CSAE	100	100
1.3	Szkolenia z prowadzenia postępowań w postaci przyjaznej dzieciom (ang. training on child-friendly investigations)	100	100
1.3.1	Narzędzia i standardy postępowania funkcjonariuszy przyjazne dzieciom, a także młodzieży (ang. child and adolescent-friendly tools and standards for investigators)	100	100
1.3.2	Przyjazne dzieciom oraz młodzieży standardy przesłuchania (ang. child and adolescent-friendly tools and standards for interviewing)	100	100
1.4	Liczba funkcjonariuszy policji na 100 000 mieszkańców (ang. Police personnel per 100 000 persons)	36	62,2

Poruszenie wątku innych państw i przeprowadzenia pełnej analizy porównawczej, chociażby w odniesieniu do przywołanego tu modelu OOSI (alternatywnie można stosować model ECPAT *Global Progress Towards Ending the Sexual Exploitation of Children* lub WeProtect Global Alliance *Model National Response to end child sexual exploitation & abuse online*), wykracza poza charakter omawianych tu zagadnień. Dlatego też jedynie zostanie zasygnalizowane, że Albania (Cami, 2024; Škorić, 2025) jest jednym z 12 krajów analizowanych w rejonie Europy i Azji (brak w tym zestawieniu Polski). W tym obszarze w tzw. TOP 5 znalazły się: Wielka Brytania, Francja, Szwecja, Turcja, Niemcy. Rozwiązania systemowe tych krajów można analizować pod kątem poszukiwania rozwiązań modelowych na potrzeby krajowe.

Na zakończenie tej części, w kontekście zagadnień związanych z tworzeniem specjalistycznych jednostek Policji, należy podkreślić, że zarówno technologia, jak i organizacja muszą mieć u podstaw zagadnienia związane z ochroną dobrostanu osób (Strickland, 2023; Bąk i in., 2024) zajmujących się służbowo analizą CSAEM

i OCSAE (analityków i moderatorów treści, biegłych, policjantów, prokuratorów czy sędziów, a także inne osoby tworzące ekosystem walki z cyberprzestępczością seksualną na szkodę dzieci). Nawiązując do tytułu jednego z artykułów poświęconych temu zagadnieniu (Conway, 2024), należy pamiętać, żeby chronić chroniących (ang. *protecting the protectors*).

Analiza przypadku – czyli CSAEM w cyber(czaso)przestrzeni

Na zakończenie artykułu w postaci *case study* zostanie omówione zagadnienie cyber(czaso)przestrzeni. Stanowi to klamrę i nawiązanie do zaprezentowanych na początku słów, gdzie zwrócono uwagę na potrzebę walidacji działań m.in. w obszarze edukacji, prawa, technologii, współpracy międzyinstytucjonalnej czy międzysektorowej, a także weryfikacji i udoskonalania języka, którym opisujemy zjawiska związane z CSAEM i OCSAE.

W tekście pt. *Wpływ czasu ujawnienia popełnienia przestępstw* autor przedstawia wyniki badań aktowych nad zagadnieniem przedawnienia karalności (art. 101 k.k.) przestępstw związanych z seksualnym wykorzystywaniem małoletnich. Jedna z jego konstatacji brzmi następująco:

> (…) upływ czasu pomiędzy zdarzeniem a zgłoszeniem tego faktu może mieć negatywny wpływ na skuteczność postępowania dowodowego. Wraz z upływem czasu obiektywny materiał dowodowy – ślady kryminalistyczne i materiały rzeczowe – ulega degradacji czy zniszczeniu. Niekiedy ma to charakter wręcz planowy – jak w przypadku danych telekomunikacyjnych, które są usuwane po upływie okresu ich retencji. Również ślady pamięciowe, co naturalne, ulegają zatarciu (Lewulis, 2025, s. 16).

Bardzo podobnie to zagadnienie przedstawia Czarnecki w odniesieniu do niemal całej rozpiętości czasowej (por. dalsze uwagi), którą należy brać pod uwagę w odniesieniu do CSAEM i OCSAE:

> (…) jeśli czas między czynem sprawcy a wydaniem rozstrzygnięcia w przedmiocie odpowiedzialności karnej jest nadmiernie długi, to trudno wówczas mówić, że takie postępowanie jest sprawiedliwe, skoro reakcja karna powinna być nieuchronna i niezwłoczna. Przedawnienie ma również istotny walor pragmatyczny, z upływem czasu zmniejsza się bowiem prawdopodobieństwo sprawnego i pełnego zgromadzenia materiału dowodowego, który może zostać wykorzystany w danym postępowaniu karnym (zob. też Czarnecki, 2023, s. 157).

W odniesieniu do cyberprzestępczości – zwłaszcza tej związanej z seksualnym wykorzystywaniem dzieci – zagadnienia temporalne mają szczególne, aczkolwiek często pomijane znaczenie. Lewulis oraz Czarnecki zwracają uwagę na czas w kontekście przedawnienia karalności. Można o nim mówić również w kontekście opóźnienia reakcji systemu (ang. *backlog*) na CSAE czy znamion przestępstw związanych z CSAEM i OCSAE. W polskim Kodeksie karnym (co w dużej mierze wynika z dostosowania tego aktu do regulacji międzynarodowych) już same formy czasownikowe czynności sprawczych pozwalają zaobserwować ponad 20 relewantnych temporalnie zmiennych, które powinny zostać uwzględnione w metodologii czynności organów ścigania i wymiaru sprawiedliwości.

Wymieńmy kilka przykładowych kodeksowych „momentów w czasie", które mogą składać się na seksualne wykorzystywanie dziecka – czy to w „klasycznej" formie kontaktowej (CSAE), czy też tej związanej z cyberprzestrzenią (CSAEM lub OCSAE). Pierwszy kontakt seksualny osoby dorosłej z dzieckiem może przybrać formę *groomingu*, zatem wiktymizacja i traumatyzacja zaczynają się, zanim dojdzie do ewentualnego przestępstwa kontaktowego. Następnie weźmy pod uwagę czas utrwalenia materiału (por. art. 202 §3, 4, 4b k.k. czy też art. 197 §3 pkt 4 w zb. z art. 197 §4 kk), czas produkcji (i postprodukcji), czas posiadania i przechowywania. Możemy dodać ponadto czas: rozpowszechniania, dystrybucji, sprowadzania, prezentowania, uzyskania dostępu. Z drugiej strony mamy czas aktywności występujących po wiktymizacji (lub jeszcze w jej trakcie), a zatem czas: ujawnienia faktu (np. w drodze reminiscencji), podjęcia decyzji o zgłoszeniu czynu i powiadomienia instytucji (np. Dyżurnet.pl, Policja, Prokuratura, PKDP), udziału w czynnościach, a następnie pożądanego przywrócenia lub chociaż poprawy dobrostanu dziecka. Z trzeciej strony należy wskazać na czas reakcji systemu (np. placówki szkolnej, Policji, Prokuratury): uzyskanie pierwszej informacji, wykonanie czynności dowodowych z małoletnim, zabezpieczenie nośników/materiałów cyfrowych, analiza cyfrowego materiału dowodowego, kategoryzacja i klasyfikacja treści (przez specjalistę Dyżurnet.pl, biegłego, Policję, Prokuraturę), kwalifikacja prawna, zakończenie postępowania (wydanie prawomocnego wyroku), realizacja kary.

Dostrzegając tę wielopoziomową cyber(czaso)przestrzeń, przyjrzyjmy się studium przypadku, w którym treści CSAEM dzięki technologiom cyfrowym zostały zmultiplikowane. Sprawca utworzył je smartfonem (paczka plików nr 1), który Policja zabezpieczyła w toku przeszukania osoby dokładnie w tym dniu. Te same pliki, bez żadnej modyfikacji, skopiował on na swój komputer stacjonarny, który służby zabezpieczyły zaraz po telefonie (paczka plików nr 2). Ostatni zbiór CSAEM (paczka plików nr 3) sprawca umieścił – w niezmienionej formie – na zlokalizowanym w Polsce

forum w tzw. otwartym internecie, skąd jeszcze przez nikogo nie został pobrany, ani obejrzany (do wątku na forum można dostać się jedynie po autoryzacji hasłem, a tego sprawca nie udostępnił z uwagi na zatrzymanie).

W oparciu o ten kazus warto zapytać: kiedy, jeżeli w ogóle, zakończyło się „posiadanie" tych treści przez sprawcę? W toku czynności zabezpieczono ww. nośniki (telefon i dysk twardy komputera z paczkami nr 1 i nr 2), a następnie potwierdzono, że w ich pamięci zostały utrwalone treści CSAEM. Można przyjąć, że czas procesowo-technicznego zabezpieczenia nośnika przez organy ścigania stanowi datę końcową „posiadania". Ten moment (data i godzina) zostanie wykorzystany przy konstruowaniu zarzutu, a następnie aktu oskarżenia.

Co jednak z paczką nr 3? Dla ułatwienia dodajmy, że treści znajdują się w zasobie sieciowym, o którym Policja wie (np. z wyjaśnień podejrzanego), że istnieje, ale nie uzyska do niego dostępu bez wprowadzenia lub złamania hasła. Ta ogólnie powszechna sytuacja rodzi problemy prawne, technologiczne i metodologiczne, których Autor tu nie rozstrzyga. Stanowią one jedynie przyczynek do dalszych rozważań metodologicznych w kontekście omówionych rozwiązań teleinformatycznych.

Wykonanie pełnej klasyfikacji zabezpieczonych treści wraz z wyliczeniem zdefiniowanych w systemie haszy (np. MD5, SHA1, PhotoDNA), a następnie zasilenie tymi danymi i informacjami specjalistycznej bazy, pozwoli zagregować pliki zawierające CSAEM i dokonać ich atrybucji (powiązać każdy jeden plik z osobą pokrzywdzoną i sprawcą). W przyszłości może to pozwolić uniknąć powtarzania czynności technicznych lub/i procesowych, a więc również wtórnej wiktymizacji (osoby pokrzywdzonej) i wtórnej traumatyzacji (analityka, biegłego itp.).

Co najmniej od 10 lat istnieją dostępne dla organów ścigania, a omówione tu pokrótce, rozwiązania pozwalające na manualne lub zautomatyzowane przeszukiwanie zasobów sieci (w tym darkwebu), takie jak *crawlery* i *scrapery* (por. opisany wcześniej Project Arachnid; IWF, 2020a, 2026). Cały zaś system ma na celu zablokowanie lub usunięcie treści. Włączenie podobnej technologii do algorytmu standardowych czynności wykrywczych może pozwolić organom ścigania i wymiarowi sprawiedliwości uniknąć powyższych dylematów, a przede wszystkim znacząco ograniczyć rozpowszechnianie treści CSAEM i tym samym chronić dzieci w najpełniejszy (proaktywny i holistyczny) sposób.

Podejście skoncentrowane na osobie pokrzywdzonej (ang. *victim-centred approach*) wymusza „odpytanie" systemu o podobnej funkcjonalności do Arachnid i bazy ICSE już w czasie realizacji czynności wstępnych. Taki przykładowy algorytm – częściowo przynajmniej rozwiązujący problem paczki nr 3 – przedstawiono poniżej. Może on być stosowany bez większych – acz zawsze pożądanych z uwagi

na różnorodność postępowań – modyfikacji zarówno do CSAE, którego skutkiem jest CSAEM/OCSAE, jak i czynów zaistniałych całkowicie w świecie wirtualnym.

1. Uzyskanie wiedzy o małoletnim/sprawcy/treściach CSAEM (takie są trzy najprostsze wektory inicjujące podjęcie działań organów ścigania i wymiaru sprawiedliwości).
2. Medyczno-psychologiczno-prawne udzielenie pomocy osobie małoletniej oraz pozyskanie – za zgodą uprawnionego podmiotu/osoby – jej wizerunku na potrzeby identyfikacji treści CSAEM.
3. Procesowo-techniczne zabezpieczenie miejsc(a) działania sprawcy, sprzętu służącego do obrazowania (np. kamery, telefony, komputery z wbudowanym urządzeniem do rejestracji multimedialnej), a także wszelkich nośników danych mogących zawierać tzw. producenckie treści CSAEM, w tym zasobów sieciowych.
4. Wstępna identyfikacja materiałów audiowizualnych z wykorzystaniem oprogramowania z funkcją tzw. wyszukiwania obrazem.
5. Przygotowanie – dla określonego podzbioru zidentyfikowanych i wyselekcjonowanych „treści producenckich" – listy haszy kryptograficznych (np. MD5, SHA1 lub nowszy) oraz tzw. haszy inteligentnych (np. PhotoDNA, Videntifier).
6. Sprawdzenie w bazie referencyjnej[8] przy użyciu ww. list haszy lub treści CSAEM, czy i w jakim charakterze znajduje się tam objęty postępowaniem materiał.
7. Sprawdzenie w systemie Arachnid/CPORT (innym posiadającym analogiczne funkcje) przy użyciu list haszy, czy i w jakim charakterze (np. czy był rozpowszechniany) znajduje się tam ww. materiał.
8. Obligatoryjne orzeczenie zniszczenia/usunięcia danych (np. pliki zawierające CSAEM, konto na forum, strona www) oraz fakultatywnie przepadku przedmiotów (np. telefon, dysk, serwer), które mają związek z popełnienia przestępstwa.
9. Prawidłowa kwalifikacja prawna (por. matryca sprawców).
10. Zakończenie postępowania.

Niezastosowanie pkt 6 i 7 może doprowadzić do sytuacji, w której zmultiplikowany przez sprawcę (lub osoby z nim powiązane) materiał CSAEM – po raz pierwszy zidentyfikowany w ramach tego postępowania – szybko rozprzestrzeni się

8 W odniesieniu do pkt 6–7 algorytmu – do czasu powstania polskiego systemu teleinformatycznego obejmującego bazę hashy i bazę wizerunków – rekomendowane jest sprawdzenie (tzw. *cross-checking*) w innych bazach/systemach, do których Policja i/lub Prokuratura ma dostęp stały lub *ad hoc*, wynikający z potrzeb zapewnienia celów postępowania karnego, np. ICSE.

w sieci i „kolekcjach" innych sprawców zainteresowanych treściami przedstawiającymi seksualne wykorzystywanie dzieci, również tych z subgrupy A1 oraz z grupy C (por. część dotyczącą typologii sprawców). W efekcie niezasilanie bazy referencyjnej (np. ICSE) „polskimi" materiałami CSAEM może prowadzić do podjęcia czynności z zakresu VID przez policję/prokuraturę innego kraju. To z kolei obciąża ich systemy walki z CSAEM i OCSAE. Może się również wiązać z inicjowaniem przez zagraniczny podmiot prowadzący postępowanie międzynarodowej pomocy prawnej, która to czynność z kolei obciąży polski wymiar sprawiedliwości i organy ścigania.

Analogicznie – wykorzystanie technologii takich jak Arachnid, CPORT, ICSE – na wczesnym etapie (zaraz po powzięciu informacji przez organy ścigania) daje szansę zapobieżenia rozprzestrzenianiu się w globalnym internecie ujawnionych w Polsce tzw. producenckich treści CSAEM.

Podsumowanie. W stronę zintegrowanego systemu ochrony małoletnich przed CSAEM i OCSAE

W artykule omówiono wyzwania związane z przestępczością seksualną wobec dzieci oraz przedstawiono wybrane krajowe i międzynarodowe inicjatywy przeciwdziałające zjawiskom CSAEM i OCSAE. Szczególną uwagę poświęcono aspektom technologicznym i metodologicznym, podkreślając, że skuteczna ochrona małoletnich w środowisku cyfrowym wymaga ciągłej aktualizacji działań podejmowanych w obszarach edukacji, prawa, technologii, współpracy międzyinstytucjonalnej i międzysektorowej, a także doskonalenia terminologii opisującej te zjawiska – m.in. w odniesieniu do typologii sprawców, definicji cyber(czaso)przestrzeni czy wyznaczania i monitorowania miejsc zagrożonych w internecie (rozumianym jako przestrzeń bezprawia).

Zwalczanie CSAEM i OCSAE jako form transgranicznej, zorganizowanej cyberprzestępczości wymaga porzucenia rozproszonych, lokalnych i reaktywnych działań na rzecz podejścia systemowego, uwzględniającego nie pojedyncze dane, a wzorce dające się zauważyć zarówno w treściach CSAEM, jak i w aktywnościach przestępczych związanych z OCSAE.

Wdrożenie w Polsce rozwiązań takich jak krajowa baza CSAM oraz systemów automatyzujących wymianę informacji (np. ICSE, Arachnid, CPORT) pozwoli skrócić czas reakcji instytucji, ograniczyć dalszą dystrybucję materiałów i zmniejszyć ryzyko wtórnej wiktymizacji. Odpowiednio zaprojektowane technologie odciążą analityków i biegłych, redukując ich ekspozycję na treści traumatyzujące. Oparte na haszach i predykcji AI rozpoznawanie znanych materiałów zwiększy skuteczność

specjalistów w identyfikacji pokrzywdzonych (VID). Budowa i pełne wykorzystanie krajowych oraz międzynarodowych baz CSAM umożliwi przejście od działań fragmentarycznych do spójnego, holistycznego mechanizmu, który zapewni proaktywną i szybką ochronę dzieci w coraz bardziej złożonej cyber(czaso)przestrzeni.

E-mail autora: **pawel.oberszt@nask.pl**

Bibliografia

Adler, A. (2001). The Perverse Law of Child Pornography. *Columbia Law Review*, 101(2), 209–273. https://doi.org/10.2307/1123799

Aiken, M., Moran, M., Berry, M.J. (2011). *Child abuse material and the Internet. Cyberpsychology of online child-related sex offending*. Referat zaprezentowany 5–7 września 2011 r. na 29 Meeting of the INTERPOL Specialist Group on Crimes against Children, Lyon, Francja. https://www.researchgate.net/publication/277774727_Aiken_Moran_Berry_2011

Ali, S., Paash, A.S. (2021). A systematic review of the technology-enabled child sexual abuse (OCSA) and its impacts. *Journal of Legal, Ethical and Regulatory Issues*, 25 (5S), 1–18. https://www.abacademies.org/articles/a-systematic-review-of-the-technology-enabled-child-sexual-abuse-ocsa-its-impacts-14884.html

Alrwais, S.A., Liao, X., Mi, X., Wang, P., Wang, X., Qian, F., Beyah, R.A., McCoy, D. (2017). *Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks*. 2017 IEEE Symposium on Security and Privacy (SP), 805–823. https://doi.org/10.1109/SP.2017.32

Bąk, G., Ogińska-Bulik, N. (2024). *Wtórna traumatyzacja wśród funkcjonariuszy policji. Konsekwencje i uwarunkowania*. Difin.

Bielawski, R. (2020). Zakres przedmiotowo-podmiotowy przestępczości zorganizowanej. *Zeszyty Naukowe Pro Publico Bono*, 1(1), 13–21. https://doi.org/10.5604/01.3001.0014.4642

Billuart, J., Gemignani, R., Perrot, P. (2025). ODIP. A state-of-the-art child sexual abuse material detection model. W D. Verdejo, E. Mercier-Laurent (red.), *AI4GS 2024. IFIP Advances in Information and Communication Technology*, 743 (18–27). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-031-96522-7_2

Billuart, J., Gemignani, R., Perrot, P. (2025). ODIP. A State-of-the-Art Child Sexual Abuse Material Detection Model. W Verdejo, D., Mercier-Laurent, E. (red.) *Artificial Intelligence for Global Security. AI4GS 2024. IFIP Advances in Information and Communication Technology*, 743 (18–27). Springer, Cham. https://doi.org/10.1007/978-3-319-14289-0_12

Bocheński, M. (2015). Ile pedofilii w „pedofilach"? Wybrane problemy wykorzystywania seksualnego małoletnich w Polsce – perspektywa kryminologiczna. *Dziecko Krzywdzone. Teoria, badania, praktyka*, 14, 199–132. https://dzieckokrzywdzone.fdds.pl/index.php/DK/article/view/471/337

Breitinger, F., Liu, H., Winter, C., Baier, H., Rybalchenko, A., Steinebach, M. (2013). Towards a process model for hash functions in digital forensics. Gladyshev, P.,

Marrington, A., Baggili, I. (red.). *Digital forensics and cyber crime: ICDF2C 2013* (170–186). Springer. https://doi.org/10.1007/978-3-319-08545-7_12

Bongen, R., Moßbrucker, D., Güldenring, B., Lenz, P. (22.04.2021). Private Kinderfotos auf Pädosexuellen-Seiten. *Tagesschau*. https://www.tagesschau.de/investigativ/panorama/kinderfotos-sozialemedien-paedosexuelle-101.html

Brown, R. (2023). *Eliminating online child sexual abuse material*. Routledge.

Brown, R., Oldenburg, E., Cole., J. (2018). Project VIC. Helping to Identify and Rescue Children from Sexual Exploitation. *Police Chief Online*. https://www.policechiefmagazine.org/project-vic

Bursztein, E., Clarke, E., DeLaune, M., Elifff, D. M., Hsu, N., Olson, L., Shehan, J., Thakur, M., Thomas, K., Bright, T. (2019). Rethinking the detection of child sexual abuse imagery on the internet. *Proceedings of the World Wide Web Conference (WWW'19)*, 2601–2607. https://doi.org/10.1145/3308558.3313482

C3P (2023). *Project Arachnid CSAM online availability*. https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability.

C3P (2026). *Project Arachnid*. https://www.projectarachnid.ca

Caffo, E. (red.). (2021). O*nline child sexual exploitation. Treatment and prevention of abuse in a digital world*. Springer.

Caianiello, M., Camon, A. (red.). (2021). *Digital forensic evidence*. Wolters Kluwer.

CameraForensics (8 lipca 2025). *The reality of organised ritual abuse – extreme abuse hidden from view*. https://www.cameraforensics.com/blog/2025/07/08/the-reality-of-organised-ritual-abuse/

Cami, G. (2024). Legal Standards for Cross-Border Access to Electronic Evidence in Criminal Procedure. An Albanian Perspective on International Standards. *Studia Iuridica Lublinensia*, 33(5), 11–30. http://dx.doi.org/10.17951/sil.2024.33.5.11-30

Casey, E. (2010). Handbook of digital forensics and investigation. Elsevier Academic Press.

Celiksoy, E., Schwarz, K. (2023). *Investigation into financial transactions used in the online sexual exploitation of children. The state of evidence*. University of Nottingham, Rights Lab. https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/investigation-into-financial-transactions-used-in-the-online-sexual-exploitation-of-children.pdf

Chau, K. (2022). *Initial results of the Tech Coalition video hash interoperability alpha project*. https://technologycoalition.org/blog/initial-results-of-the-tech-coalition-video-hash-interoperability-alpha-project

Childlight (2025a). *2025 into the light index on global child sexual exploitation and abuse. Supplemental thematic analysis report*. Childlight – Global Child Safety Institute. https://www.childlight.org/uploads/publications/intothelight2025/STAR_2025.pdf

Childlight (2025b). *Who benefits? Shining a Light on the Business of Child Sexual Exploitation and Abuse*. https://www.childlight.org/uploads/publications/searchlight2025/Childlight_Searchlight_Report_2025.pdf

Childlight (2025c). *Global experts call for new approach to protect children from 'pandemic' of sexual exploitation and abuse*. https://www.childlight.org/newsroom/global-experts-call-for-new-approach-to-protect-children-from-pandemic-of-sexual-exploitation-and-abuse

Chlebowicz, P., Łabuz, P., Safjański, T. (red.). (2022). *Antykryminalistyka. Taktyka i technika działań kontrwykrywczych*. Difin.

Chojnowski, A. (2020). *Informatyka sądowa w praktyce*. Helion.

CLKP. (2018). *Stanowisko dostępowe do bazy ICSE (Interpol) w pracowni informatyki śledczej CLKP*. https://clkp.policja.pl/clk/informatyka-sledcza-w-c/miedzynarodowa-wymiana/158734,Stanowisko-dostepowe-do-bazy-ICSE-Interpol-w-pracowni-informatyki-sledczej-CLKP.html

Conway, P., Redmond, T., Lundrigan, S., Davy, D., Bailey, S., Lee, P. (2024). Protecting the protectors. Moral injury, coping styles, and mental health of UK police officers and staff investigating child sexual abuse material. *Depression and Anxiety*, 2024. https://doi.org/10.1155/da/1854312

CyberDefence24 (17.09.2025). *Rząd stworzy nowy system do walki z wykorzystywaniem dzieci*. https://cyberdefence24.pl/cyberbezpieczenstwo/rzad-stworzy-nowy-system-do-walki-z-wykorzystywaniem-dzieci

Czarnecki, P. (2023). *Przedawnienie i zatarcie skazania przestępstw przeciwko wolności seksualnej – między surowym ukaraniem sprawcy a ochroną interesów małoletniego pokrzywdzonego*. Dziecko Krzywdzone. Teoria, badanie, praktyka, 22, 152–184. https://dzieckokrzywdzone.fdds.pl/index.php/DK/article/view/876/721

Dąbrowska, M. (2025). Propozycja reform terminologicznych dotyczących kryminalizacji materiałów przedstawiających wykorzystywanie seksualne małoletnich (CSAM) w polskim prawie karnym. *Studia Prawnoustrojowe*, 68, 47–67. https://doi.org/10.31648/sp.11036

Daskalaki, E., Kokolaki, E., Fragopoulou, P. (2025). Hashing in the Fight Against CSAM. Technology at the Crossroads of Law and Ethics. *Journal of Cybersecurity and Privacy*, 5(4), 92, 1–20. https://doi.org/10.3390/jcp5040092

Davis, P. (2025). *Spike in online crimes against children a „wake-up call"*. National Center for Missing & Exploited Children. https://www.missingkids.org/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call

Demidova, E. (2021). The concept of forensic activity (ontological aspect). W D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz, E.W. Pływaczewski (red.). *Przestępczość XXI wieku. Szanse i wyzwania dla kryminologii* (467–476). Wolters Kluwer.

Deutsche Welle (2021, 13 grudnia). *German court jails operators of darknet cyber hub*. https://www.dw.com/en/german-court-jails-operators-of-darknet-cyber-hub/a-60104450

Dolniak, P., Kuźma, T., Ludwiński, A., Wasik, K. (2024). *Sztuczna inteligencja w wymiarze sprawiedliwości. Między prawem a algorytmami*. Wolters Kluwer.

Durkin, K., DeLong, R. (2012). Internet crimes against children. W Yan Z. (Ed.), *Encyclopedia of cyber behavior*. IGI Global. https://doi.org/10.4018/978-1-4666-0315-8.ch066

Dyżurnet.pl (2021). *Cyfrowy ślad małego dziecka*. NASK PIB. https://dyzurnet.pl/uploads/2021/07/Cyfrowy_slad_malego_dziecka.pdf

Dyżurnet.pl. (2026). Raport 2026. https://dyzurnet.pl/publikacje

ECPAT (2025a). *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse* (wyd. 2). https://ecpat.org/wp-content/uploads/2025/04/Second-Edition-Terminology-Guidelines-final.pdf

ECPAT (2025b). https://ecpat.org/our-impact/

Elshenraki, H.N. (red.). (2021). *Combating the exploitation of children in cyberspace: Emerging research and opportunities*. IGI Global.

Europol (2015). *IOCTA 2014*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2014

Europol (2021). *IOCTA 2020*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Europol (2025a). *25 arrested in global hit against AI-generated child sexual abuse material*. https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

Europol (2025b). *Analysis Project TWINS (AP TWINS)*. https://www.europol.europa.eu/how-we-work/europol-analysis-projects

Europol (2025c). *Victim Identification Task Force (VIDTF)*. https://www.europol.europa.eu/media-press/newsroom?q=VIDTF

Europol (2025d). *From streets to screens. Fighting crime in the digital domain*. https://www.europol.europa.eu/media-press/newsroom/news/streets-to-screens-fighting-crime-in-digital-domain

Farid, H. (2018). Reining in online abuses. *Technology and Innovation*, 19, 593–599. https://farid.berkeley.edu/downloads/publications/nai18.pdf

Farid, H. (2021). An overview of perceptual hashing. *Journal of Online Trust and Safety*, 1–22. https://tsjournal.org/index.php/jots/article/view/24

Ferraro, M.M., Casey, E. (2004). *Investigating child exploitation and pornography. The Internet, law and forensic science*. Academic Press.

Fortin, F., Paquette, S., Gagné, S. (2021). Challenges and opportunities in investigations of online sexual exploitation of children. Old networks, dark web, and proactive response. W Deslauriers-Varin, N., Bennell, C. (red.). *Criminal investigations of sexual offenses. Techniques and challenges*. https://doi.org/10.1007/978-3-030-79968-7_15

Francis, F., Sarah, P., Stephanie, G., Nadine, D.V., Craig, B. (2021). Challenges and opportunities in investigations of online sexual exploitation of children. Old networks, dark web, and proactive response. W *Criminal investigations of sexual offenses. Techniques and challenges* (217–233). Springer. https://doi.org/10.1007/978-3-030-79968-7_15

García-Retuerta, D., Bartolomé, Á., Chamoso, P., Corchado, J.M. (2019). Counter-Terrorism Video Analysis Using Hash-Based Algorithms. *Algorithms*, 12, 110, 1–9. https://doi.org/10.3390/a12050110

Gless, S. (2020). AI in the courtroom. A comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law*, 51(2), 195–256. https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2020/05/GT-GJIL200024.pdf

Google (2023). *Transparency report*. https://transparencyreport.google.com/child-sexual-abuse-material/reporting?lu=total_content_reported&total_content_reported=period:2021H2&total_accounts_disabled=period:2020H1&top_ten_accounts_disabled_countries=period:2022H2

Google (2025). *What makes the CSAI Match technology so efficient?* https://protectingchildren.google/tools-for-partners/#learn-about-our-tools

Google (2026). *Transparency report 2025 (1)*. https://transparencyreport.google.com/child-sexual-abuse-material/reporting?lu=total_content_reported&total_content_reported=period:2025H1;detectionmethod:DETECTION_METHOD_MANUAL&total_accounts_disabled=period:2020H1&top_ten_accounts_disabled_countries=period:2025H1&hl=en

ForensicsFocus (2018, 24 maja). *Griffeye releases new AI technology trained to aid child abuse investigations*. https://www.forensicfocus.com/news/griffeye-releases-new-ai-technology-trained-to-aid-child-abuse-investigations/

Grossman, S., Pfefferkorn, R., Thiel, D., Shah, S., DiResta, R., Perrino, J., Cryst, E., Stamos, A., Hancock, J. (2024). *The Strengths and Weaknesses of the Online Child Safety Ecosystem*. Stanford Digital Repository. https://doi.org/10.25740/pr592kc5483

HashSets.com (2026). *White Hash Set*. https://www.hashsets.com/

HMICFRS (2023). *An inspection of how well the police and National Crime Agency tackle the online sexual abuse and exploitation of children*. https://hmicfrs.justiceinspectorates.gov.uk/publication-html/inspection-of-how-well-police-and-national-crime-agency-tackle-online-sexual-abuse-and-exploitation-of-children/

Homeland Security (2014). *X-Ways Forensics v17.6 Test Results for Graphic File Carving Tool*. https://www.dhs.gov/sites/default/files/publications/508_Test%20Report_NIST_X-Ways%20Forensics%20v17.6_0_August%202015_Final_0.pdf

Hydrant Programm (2024). *Group-Based Offending Publication*. https://www.hydrant-programme.co.uk/assets/Documents/CSE-Taskforce-Group-Based-Offending-Publication-November-2024.pdf

ICMEC (2021). *Cryptocurrency and the trade of online child sexual abuse materia*. https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf

INHOPE (2024). *Global CSAM legislative overview 2024*. https://inhope.org/media/pages/action-awareness/publications/publications/ba55a6bce2-1765563872/global-csam-legislative-overview-2024-full-report.pdf

INHOPE (2025a). *Binance partners with INHOPE to fight online abuse*. https://inhope.org/articles/binance-partners-with-inhope-to-fight-online-abuse

INHOPE (2025b). *The Universal Classification Schema*. https://universalclassification-schema.org/

INHOPE (2025c). *Webinar Recap. The INHOPE Annual Report 2024*. https://inhope.org/articles/webinar-recap-the-inhope-annual-report-2024

Interpol (2018). *Technical report - Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material*. https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Interpol (2022a). *More specialist units needed to investigate online child abuse*. https://www.interpol.int/News-and-Events/News/2022/INTERPOL-Secretary-General-More-specialist-units-needed-to-investigate-online-child-abuse

Interpol (2022b). *2022 Interpol Global Crime Trend Summary Report*. https://www.interpol.int/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

Interpol (2023). *Blocking and categorizing content*. https://www.interpol.int/Crimes/Crimes-against-children/Blocking-and-categorizing-content

Interpol (2024). *Resolution No. 5*. https://www.interpol.int/content/download/22199/file/GA-2024-92-RES-05%2520E%2520Agreement%2520IWOL.pdf

Interpol (2025). *International Child Sexual Exploitation database (ICSEdb)*. https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

IWF (2020). *Case Studie. Three year old Amy seen three times a day*. https://annualreport2020.iwf.org.uk/trends/casestudies/amy

IWF (2020a). *Crawler*. https://annualreport2020.iwf.org.uk/tech/new/crawlers

IWF (2021). *IntelliGrade*. https://www.iwf.org.uk/our-technology/intelligrade/

IWF (2023). *How AI is being abused to create child sexual abuse imagery*. https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf

IWF (2024). *What has changed in the AI CSAM landscape?* https://admin.iwf.org.uk/media/nadlcb1z/iwf-ai-csam-report_update-public-jul24v13.pdf

IWF (2026). *Crawler*. https://www.iwf.org.uk/our-technology/crawler/

Kamar, E., Liggett O'Malley, R., Howell, C.J., Maimon, D., Shabat, D. (2025). „Cutie, click on the link". A forensic analysis of URLs. *Computers in Human Behavior*, 162, 1–9. https://doi.org/10.1016/j.chb.2024.108454

Kasprzak, W. (2015). *Ślady cyfrowe*. Difin.

Kavruk Erdim, N., Bas, G. (2026). Adolescent online child sexual abuse material offending in Turkey. Psychosocial and forensic profiles from NCMEC reports and child protection implications. *Child Abuse & Neglect*, 172, 1–11. https://doi.org/10.1016/j.chiabu.2025.107851

Kemal, K.A. (2019). Framework for a single global repository of child abuse materials. *Global Policy*, 11(1), 178–190. https://doi.org/10.1111/1758-5899.12739

Kierznowski, W. (2025). Wybrane obszary działalności zorganizowanych grup przestępczych w Polsce. *Kortowski Przegląd Prawniczy*, 2, 17–27. https://doi.org/10.31648/kpp.11347

Kowalski, B., Radziszewski, R. (2017). Ekspertyza informatyczna. W Kała M., Wilk D., Wójcikiewicz J. (red.). *Ekspertyza sądowa. Zagadnienia wybrane* (634–673). Wolters Kluwer.

KPRM (2023). *Uchwała w sprawie przyjęcia Krajowego Planu Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich*

na lata 2023–2026. https://www.gov.pl/web/premier/uchwala-w-sprawie-przyjecia-krajowego-planu-przeciwdzialania-przestepstwom-przeciwko-wolnosci-seksualnej-i-obyczajnosci-na-szkode-maloletnich-na-lata-2023-2026

KPRM (2025). *Projekt ustawy o krajowym systemie przetwarzania, analizy i klasyfikacji treści przedstawiających seksualne wykorzystywanie małoletnich*. https://www.gov.pl/web/premier/projekt-ustawy-o-krajowym-systemie-przetwarzania-analizy-i-klasyfikacji-tresci-przedstawiajacych-seksualne-wykorzystywanie-maloletnich

Krać-Batyra, A., Oberszt, P., Sidor T. (2025). Interdyscyplinarne spojrzenie na problematykę komunikacji dzieci w cyberprzestrzeni z uwzględnieniem zagadnienia wytwarzania i wymiany nielegalnych treści przedstawiających osoby małoletnie. *Dziecko Krzywdzone. Teoria, badania, praktyka*, 24(1), 59–102. https://dzieckokrzywdzone.fdds.pl/index.php/DK/article/view/956

Kumar, S., Saxena, G. (2021). Child online pornography. Criminal methods and investigation. W Elshenraki, H.N. (red.). *Combating the exploitation of children in cyberspace. Emerging research and opportunities* (117–145). IGI Global. https://doi.org/10.4018/978-1-7998-2360-5.ch006

Lazarus, L., Le Toquin, J.C., Magriço Aires, M., Nunes, F., Staciwa, K., Vermeulen, G., Walden, I., Sicilianos, L.A. (2021). *Respecting human rights and the rule of law when using automated technology to detect online child sexual exploitation and abuse*. Council of Europe. https://rm.coe.int/respecting-human-rights-and-the-rule-of-law-when-using-automated-techn/1680a2f5ee

Lee, H.E., Ermakova, T., Ververis, V., Fabian, B. (2020). Detecting child sexual abuse material. A comprehensive survey. Forensic Science International. *Digital Investigation*, 34, 1–11. https://doi.org/10.1016/j.fsidi.2020.301022

Lewulis, P. (2021). *Dowody cyfrowe. Teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*. Wydawnictwa Uniwersytetu Warszawskiego.

Lewulis, P. (2025). *Wpływ czasu ujawnienia popełnienia przestępstw*. Instytut Wymiaru Sprawiedliwości.

Macedo, J., Laranjeira, C., Ribeiro, L.S.F., Caetano, C., Benevenuto, F., Avila, S., dos Santos, J.A. (2025). *Child sexual abuse datasets. A systematic review* (Preprint). Research Square, 1–20. https://www.researchsquare.com/article/rs-7963252/v1

Macilotti, G. (2020). Online child pornography. Conceptual issues and law enforcement challenges. W Balloni, A. Sette, R. (red.). *Handbook of research on trends and issues in crime prevention, rehabilitation, and victim support* (226–247). IGI Global.

Majed, H., Noura, H., Chehab, A. (2020). Overview of digital forensics and anti-forensics techniques. W *Proceedings of the International Symposium on Digital Forensics and Security (ISDFS)* (1–5). https://doi.org/10.1109/ISDFS49300.2020.9116399

Martellozzo, E. (2012). *Online child sexual abuse grooming. Policing and child protection in a multi-media world*. Routledge.

McKeown, S., Russell, G., Leimich, P. (2019). Fast forensic triage using centralised thumbnail caches on Windows operating systems. *Journal of Digital Forensics, Security and Law*, 14(3), 1–21. https://doi.org/10.15394/jdfsl.2019.1591

Morales, F., Sharma, S., Doan, C., Levine, B. (2024). *PHVSpec. A benchmark-based analysis of perceptual hash systems for videos*. https://technologycoalition.org/wp-content/uploads/Tech-Coalition-Video-Hash-Benchmark-Paper.pdf

Moszczyński, J. (2020). Kryminalistyczne bazy danych. W Goc M., Gruza E., Moszczyński J. (red.). *Kryminalistyka. Czyli o współczesnych metodach dowodzenia przestępstw* (703–710). Wolters Kluwer.

Nabokov, V. (2024). *Lolita*. Tłum. M. Kłobukowski. W.A.B.

NASK (2019). *Doświadczenia zawodowe i przekonania biegłych sądowych w sprawach związanych z materiałami przedstawiającymi seksualne wykorzystanie dziecka (raport niepublikowany)*. Naukowa i Akademicka Sieć Komputerowa PIB.

NCMEC (2025). *Global Platform for Child Exploitation Policy (GPCEP). Data insights*. https://www.globalchildexploitationpolicy.org/data-insights

Nijakowski, L.M. (2010). *Pornografia. Historia, znaczenie, gatunki*. Wydawnictwo Iskry.

NIST (2015). *Test Results for Disk Imaging Tool. X-Ways Forensics Version 18.8*. http://1www.x-ways.net/imager/NIST_Test_Results.pdf

NIST (2026). *National Institute of Standards and Technology (NIST) – National Software Reference Library (NSRL)*. https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/nsrl-download/current-rds)

NPCC (2022). *The Hydrant Programme*. https://www.npcc.police.uk/our-work/work-of-npcc-committees/Crime-Operations-coordination-committee/hydrant-programme/

OCCRP (2023). *INTERPOL Operation Dismantles Global Child Abuse Networks*. https://www.occrp.org/en/news/interpol-operation-dismantles-global-child-abuse-networks

OECD (2023). *Transparency reporting on child sexual exploitation and abuse online*. https://doi.org/10.1787/554ad91f-en

OECD (2025). *Transparency reporting on child sexual exploitation and abuse online*. https://doi.org/10.1787/a89e3f08-en

Oettinger, W. (2023). *Informatyka śledcza. Gromadzenie, analiza i zabezpieczanie dowodów elektronicznych dla początkujących* (wyd. 2). Helion.

Ofcom (2022). *Overview of perceptual hashing technology*. https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/other/perceptual-hashing-technology.pdf?v=328806

Out of The Shadows (2022). *Global OOSI Index*. https://outoftheshadows.global/data

Pużyński, S., Wciórka, J. (1998). *Międzynarodowa Statystyczna Klasyfikacja Chorób i Problemów Zdrowotnych. Rewizja dziesiąta. Klasyfikacja zaburzeń psychicznych i zaburzeń zachowania w ICD-10. Badawcze kryteria diagnostyczne*. Vesalius.

Pużyński, S., Wciórka, J. (2000). *Klasyfikacja zaburzeń psychicznych i zaburzeń zachowania w ICD-10. Opisy kliniczne i wskazówki diagnostyczne*. Vesalius.

Quayle, E., Ribisl, K. (red.). (2012). *Understanding and preventing online sexual exploitation of children*. Routledge.

Ramesh Babu, B., Usha Rani, T., Naga Kumari, Y.V. (2024). AI's Watchful Eye: Protecting Children from Sexual Abuse with Artificial Intelligence. W Shaik, A., Thota, S.L., Atmakuri, L.R. (red.) *Child Sexual Abuse*. Springer, https://doi.org/10.1007/978-981-99-8745-0_37

Rogers, M., Piper, M., Bates, S. (2023). A brief history of digital forensics and digital evidence. W *Encyclopedia of forensic sciences* (wyd. 3, t. 1, s. 10). Elsevier.

Rosli, N., Dusuki, F.N. (2018). The historical development of the laws relating to child sexual exploitation prior to the passing of the UNCRC in 1989. *International Journal of Law, Government and Communication*, 8(11), 968–973. https://ideas.repec.org/a/asi/ijoass/v8y2018i11p968-973id3059.html

Roth, A.L. (2017). Machine testimony. *Yale Law Journal*, 126, 1972–2042. https://www.yalelawjournal.org/pdf/RothFinal_c4o97on1.pdf](https://www.yalelawjournal.org/pdf/RothFinal_c4o97on1.pdf

Safeguarding Childhood (2025). *An Assessment of National Budgeting Transparency to Prevent and Respond to Child Sexual Abuse*. https://safeguardingchildhood.com

Sajkowska, M. (2003). Przekazy prasowe na temat wykorzystywania seksualnego dzieci – „stare" i „nowe" historie. *Dziecko Krzywdzone. Teoria, badania, praktyka* (5), 1–15. https://testdzieckokrzywdzone.fdds.pl/index.php/DK/article/view/141/110

Sanchez, L., Grajeda, C., Baggili, I., Hall, C. (2019). A practitioner survey exploring the value of forensic tools, AI, filtering and safer presentation for investigating child sexual abuse material. *Digital Investigation*, 29 (Suppl.), 124–142. https://doi.org/10.1016/j.diin.2019.04.005

Seigfried-Spellar, K. (2018). Assessing the psychological well-being and coping mechanisms of law enforcement investigators vs. digital forensic examiners of child pornography investigations. *Journal of Police and Criminal Psychology*, 33(3), 215–226. https://link.springer.com/article/10.1007/s11896-017-9248-7

Shavers, B., Larson, T., Yasumoto, M. (red.). (2022). *X-Ways Forensics Practitioner's Guide* (wyd. 2). DFIR Training.

Škorić, J. (2025). *Towards uniformed legislation against CSAM – Western Balkan countries (Republic of Serbia, Republic of Albania and North Macedonia)*. Centre for Missing and Exploited Children, Republic of Serbia. https://www.childrensembassy.org.mk/content/TOMAS%20-%20Regional%20paper-ENG%20(4).pdf

Solanke, A.A. (2022). Digital forensics AI. Evaluating, standardizing and optimizing digital evidence mining techniques. *Künstliche Intelligenz*, 36, 135–145. https://doi.org/10.1007/s13218-022-00763-9

Steel, C.M.S., Newman, E., O'Rourke, S., Quayle, E. (2021). Collecting and viewing behaviors of child sexual exploitation material offenders. *Child Abuse & Neglect*, 118. https://doi.org/10.1016/j.chiabu.2021.105133

Steel, C., Newman, E., O'Rourke, S., Quayle, E. (2022). Lawless space theory for online child sexual exploitation material offending. *Aggression and Violent Behavior*, 68, 1–13. https://doi.org/10.1016/j.avb.2022.101809

Stoykova, R. (2021). Digital evidence. Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, 1–20. https://doi.org/10.1016/j.clsr.2021.105575

Strickland, C., Kloess, J.A., Larkin, M. (2023). An exploration of the personal experiences of digital forensics analysts who work with child sexual abuse material on a daily basis. „You cannot unsee the darker side of life". *Frontiers in Psychology*, 14, 1–10. https://doi.org/10.3389/fpsyg.2023.1142106

Sunde, N. (2022). *Constructing digital evidence. A study on how cognitive and human factors affect digital evidence. (doctoral dissertation)*. University of Oslo. https://www.duo.uio.no/handle/10852/97851

Szmit, M. (2014). *Wybrane zagadnienia opiniowania sądowo-informatycznego*. Polskie Towarzystwo Informatyczne.

Tech Coalition (2022). *Child sexual abuse material (CSAM). Identification and reporting for U.S.-based companies*. https://technologycoalition.org/wp-content/uploads/CSAM-Identification_Reporting_R3-1.pdf

Tech Coalition (2023). *Announcing Lantern. The first child safety cross-platform signal sharing program*. https://technologycoalition.org/news/announcing-lantern

Tech Coalition (2025a). *Building bridges between hash systems to combat CSAM*. https://technologycoalition.org/news/building-bridges-between-hash-systems-to-combat-csam

Tech Coalition (2025b). *Lantern Transparency Report 2024*. https://technologycoalition.org/wp-content/uploads/lantern-transparency-report_2024.pdf

Tech Coalition (2025c). *Annual Report 2024*. https://technologycoalition.org/wp-content/uploads/Tech-Coalition-Annual-Report-2024.pdf

TheFinancialCrimeNews.com. (2021). https://thefinancialcrimenews.com/wp-content/uploads/2021/07/Germany-2021-Final-Pbd-V3.pdf

Thiel, D., Stroebel, M., i Portnoff, R. (2023). *Generative ML and CSAM. Implications and mitigations*. https://fsi.stanford.edu/publication/generative-ml-and-csam-implications-and-mitigations

Thorn (2023). *How hashing and matching can help prevent revictimization*. https://www.thorn.org/blog/hashing-detect-child-sex-abuse-imagery

Thorn (2024). *Mitigating the risk of generative AI models creating child sexual abuse materials*. https://partnershiponai.org/wp-content/uploads/2024/11/case-study-thorn.pdf

Thorn. WeProtect (2024). *Evolving technologies horizon scan. A review of technologies carrying notable risk and opportunity in the fight against technology-facilitated child sexual exploitation*. https://info.thorn.org/hubfs/Research/Thorn_x_WPGA_EvolvingTechnologies_Dec2024.pdf

Tselenti, D., Carvalho, J., Azevedo, V., Gomes, H.S., Haubrock, L.S., Hillert, J., Rahm, C., Briken, P., Dekker, A., Joleby, M., Seto, M.C. (2025). Policing child sexual exploitation and abuse cases. A qualitative PRIORITY study of the challenges faced by law enforcement officers in Germany, Portugal, and Sweden. *Policing and Society*. https://www.tandfonline.com/doi/full/10.1080/10439463.2024.2447842

UK.GOV (2024). *Guidance. Child abuse image database (CAID)*. https://www.gov.uk/government/publications/child-abuse-image-database/child-abuse-image-database-caid-privacy-notice#the-road-ahead

UK.GOV. (2025). *Policy paper. Crime and Policing Bill. Child sexual abuse material factsheet*. https://www.gov.uk/government/publications/crime-and-policing-bill-2025-factsheets/crime-and-policing-bill-child-sexual-abuse-material-factsheet

UNICEF Innocenti (2025, 23 maja). *Beyond algorithms. Three signals of changing AI-child interaction. How AI chatbots may change the way children grow up*. https://www.unicef.org/innocenti/stories/beyond-algorithms-three-signals-changing-ai-child-interaction

Van De Sandt, E. (2019). *Deviant security. The technical computer security practices of cyber criminals (doctoral dissertation)*. University of Bristol. https://research-information.bris.ac.uk/en/studentTheses/deviant-security

WeProtect Global Alliance (2025). *WeProtect Global Threat Assessment 2025*. https://www.weprotect.org/wp-content/uploads/GTA-2025_EN.pdf

Wilkowski, A. (2025). Metody rozpoznawania aktywności w sekwencjach wideo przy użyciu niskopoziomowych cech obrazu. *Cybersecurity and Law*, 1(13), 181–196. https://www.cybersecurityandlaw.pl/nr-1/17.pdf

Wolbers, H., Cubitt, T., Cahill, M.J. (2025). *Artificial intelligence and child sexual abuse. A rapid evidence assessment. Trends & Issues in Crime and Criminal Justice*. Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2025-01/ti711_artificial_intelligence_and_child_sexual_abuse.pdf

ZIUZ (2023a). *Vizx*. https://www.ziuz.com/content/uploads/2022/05/V2-Vizxbrochure-dark-background_compressed-2.pdf

ZIUZ (2023b). *Fenzoz*. https://www.ziuz.com/try-fenoz-image-module/

ZIUZ (2023c). *Cortado AI*. https://www.ziuz.com/de/products/cortado/

Combating Child Sexual Abuse & Exploitation in Cyberspace: CSAEM, OCSAE, and Emerging Technological & Methodological Challenges

Protecting children from organized, transnational cybercrime is a complex issue. It requires continuous validation of actions undertaken in areas such as education, law, technology, inter-institutional and cross-sector cooperation, as well as ongoing refinement of the conceptual framework used to describe related phenomena. The article focuses on selected technological challenges, within the discussion of which several methodological issues related to combating child sexual abuse are also addressed, with particular emphasis on CSAEM (Child Sexual Abuse & Exploitation Materials) and OCSAE (Online Child Sexual Abuse & Exploitation).

CSAEM may constitute evidence of real, traumatizing events or be modified and/or fully digitally generated. OCSAE represents a form of cybercrime targeting minors, the effective mitigation of which requires, on the one hand, an adequate offender taxonomy and, on the other, the use of increasingly advanced solutions enabling the effective detection and preservation of evidence of such prohibited acts online. Modern digital tools – such as specialized software, CSAM databases (containing, among other things, files depicting victims, their categorization, and hashes), information-sharing platforms, crawlers and scrapers, as well as AI-based solutions – enable the processing of terabytes or even petabytes of digital data with precision and at least semi-automated efficiency. The results obtained (including predictive outputs such as content categorization, victim identification, or geolocation) accelerate the acquisition of evidence relevant to investigative procedures, reduce exposure time to CSAEM, and, above all, facilitate the discovery of previously unknown materials depicting the sexual exploitation of minors, which may ultimately lead to identifying the children themselves.

The central premise of the article is that implementing functionally analogous solutions in Poland would strengthen national and international cooperation between law enforcement, the judiciary, the INHOPE hotline network – including the Polish hotline Dyżurnet.pl operated by NASK PIB – as well as Internet Content Providers (ICP) and Internet Service Providers (ISP), thereby contributing to more effective protection of the youngest users of cyberspace.

Keywords:
CSAM, CSAEM; OCSAE; child protection; organized cybercrime; technology

Cytowanie:
Oberszt, P. (2026). Zwalczanie seksualnego wykorzystywania dzieci w internecie na przykładzie CSAEM i OCSAE. Wyzwania technologiczne i metodologiczne. *Dziecko Krzywdzone. Teoria, badania, praktyka*, 25(1), 81–146.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości