dyżurnet.pl NASK

CSIRT NASK

RAPORT 2025

RAPORT 2025

dyżurnet.pl NASK

CSIRT NASK

NASK

Dyżurnet.pl – Raport 2025

AUTORZY
Zespół Dyżurnet.pl

REDAKCJA JĘZYKOWA
NASK – PIB

OPRAWA GRAFICZNA
NASK – PIB

ISSN: 2084-7785

Zespół Dyżurnet.pl realizuje działania w ramach CSIRT NASK na podstawie dotacji podmiotowej

dyżurnet.pl NASK INHOPE Ministerstwo Cyfryzacji

Warszawa 2026

Spis treści

Wstęp

20 lat temu w NASK został powołany zespół Dyżurnet.pl. Była to odpowiedź na pojawiające się zgłoszenia o materiałach, które budziły niepokój użytkowników internetu i pokazywały dzieci w kontekście seksualnym. Od początku mieliśmy świadomość, że oprócz umiejętności technicznych analityków obsługujących zgłoszenia do realizowania tej misji niezbędne są także odporność psychiczna oraz wypracowanie specjalnych procedur reagowania na treści nielegalne.

Te 20 lat obfitowało w wiele zmian, które ukształtowały dzisiejszy internet. Wierzymy, że do części z nich przyczyniliśmy się swoją codzienną pracą – analizując i reagując na otrzymane zgłoszenia, a także budując świadomość na temat zagrożeń.

Z naszej perspektywy do najważniejszych zagadnień należą: penalizacja promowania pedofilii oraz zmiana języka poprzez upowszechnianie terminu „materiały przedstawiające seksualne wykorzystywanie dzieci (CSAM)". Bardzo istotne jest również podkreślanie tego, że treści nie muszą być nielegalne, aby były szkodliwe dla dzieci, a także uświadomienie społeczeństwu konieczności dostosowywania produktów cyfrowych do wieku odbiorców i zaostrzania regulacji mających na celu ochronę najmłodszych.

Nieustanny rozwój sieci i dostępnych narzędzi niesie też za sobą kolejne wyzwania, takie jak zjawisko rozpowszechniania treści seksualnych wytwarzanych przez dzieci, a w ostatnim czasie także CSAM generowany z użyciem AI.

Przez cały czas jako Dyżurnet.pl podejmujemy działania wewnętrzne, aby sprostać wymaganiom zmieniającej się rzeczywistości – rozwijamy Zespół, doskonalimy procedury reagowania oraz opracowujemy narzędzia, w tym algorytmy AI, które pomagają nam w priorytetyzacji zgłoszeń.

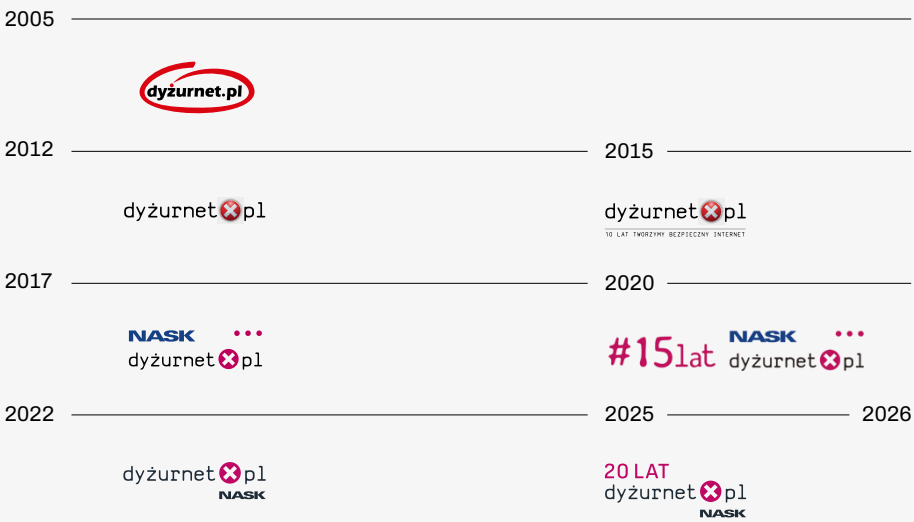
20 lat pracy to dobry moment, żeby powiedzieć o ludziach, którzy budują Zespół – Bohaterach Dnia Cogodzinnego. Z tego miejsca chylę przed nimi czoła. Nic by się nie wydarzyło bez ich wysiłku, kreatywności i wytrwałości w dążeniu do tego, aby internet był bezpieczniejszy, a sprawcy czynów

zabronionych ponosili konsekwencje swoich działań. Każdego dnia zespół Dyżurnet.pl wkłada całe swoje serce w pracę, która jest także życiową misją.

Jednocześnie wiemy, że sami nie zmienimy świata. Nasze wysiłki nie byłyby tak skuteczne bez wsparcia wielu instytucji, organizacji oraz branży technologicznej, a także odpowiedzialnych użytkowników internetu. Dlatego dziękujemy za wszystko, co już robicie i jednocześnie prosimy o jeszcze większe zaangażowanie – zwłaszcza dziś, gdy nowe technologie są tak powszechne w życiu najmłodszych, ale wciąż nie odpowiadają w pełni na ich potrzeby. Mamy razem jeszcze wiele do zrobienia!

Z poważaniem

Martyna Różycka
Dyżurnet.pl



RYSUNEK 1. Zmiany logotypu Dyżurnet.pl na przestrzeni lat

O nas

Zespół **Dyżurnet.pl** został powołany w 2005 roku w NASK – Państwowym Instytucie Badawczym. Jest jedynym w Polsce zespołem reagującym na nielegalne i szkodliwe treści w internecie. Na podstawie **ustawy o krajowym systemie cyberbezpieczeństwa** przyjmuje zgłoszenia dotyczące dystrybucji materiałów przedstawiających seksualne wykorzystywanie dzieci. Od początku działalności **Dyżurnet.pl** należy do **Stowarzyszenia INHOPE** (https://inhope.org/). To globalna sieć, która zrzesza zespoły reagujące z różnych krajów, prowadzi współpracę z międzynarodowymi organami ścigania, m.in. z Interpolem, oraz firmami branży technologicznej. Celem Stowarzyszenia jest wsparcie krajowych hotline'ów przeciwdziałających dystrybucji materiałów przedstawiających seksualne wykorzystywanie dzieci.

Od 2005 roku zespół Dyżurnet.pl realizuje strategię Komisji Europejskiej Better Internet for Kids, **współtworząc Polskie Centrum Programu Safer Internet (PCPSI)** https://saferinternet.pl/. Tworzą je: NASK – Państwowy Instytut Badawczy (koordynator PCPSI) oraz Fundacja Dajemy Dzieciom Siłę (FDDS). Strategia, wdrożona w większości krajów europejskich (https://better-internet-for-kids.europa.eu), ma na celu promowanie bezpiecznego korzystania z internetu i nowych technologii oraz wsparcie reagowania na zagrożenia cyfrowe dotykające najmłodszych.

Dodatkowo zespół realizuje zadania Krajowego Planu Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich na lata 2023–2026.

Co warto podkreślić, dzięki współpracy z wybranymi serwisami internetowymi i portalami społecznościowymi zespół **Dyżurnet.pl** działa jako *trusted flagger*, czyli zaufany podmiot sygnalizujący. Zgłoszenia składane przez takie podmioty są traktowane przez usługodawców priorytetowo.

Jak działamy?

Dyżurnet.pl przyjmuje zgłoszenia poprzez:

formularz znajdujący się na stronie internetowej	adres mailowy	aplikację mobilną
www.dyzurnet.pl	dyzurnet@dyzurnet.pl	mObywatel

Ze względu na ryzyko poniesienia konsekwencji karnych z powodu uzyskiwania dostępu do nielegalnych treści oraz na ich szkodliwy charakter zespół Dyżurnet.pl odradza samodzielne wyszukiwanie ich w internecie.

Kategorie, które są objęte procedurą reagowania[1]:

- materiały przedstawiające seksualne wykorzystywanie dziecka: art. 202 §3, 4, 4a, 4b k.k. – prawo polskie zabrania produkowania, utrwalania, sprowadzania, rozpowszechniania, prezentowania, przechowywania, uzyskiwania dostępu oraz posiadania treści pornograficznych z udziałem małoletniego;

- materiały przedstawiające twardą pornografię: art. 202 §3 k.k. – prawo polskie zabrania rozpowszechniania i publicznego prezentowania pornografii związanej z wykorzystaniem przemocy lub posługiwaniem się zwierzęciem;

- treści propagujące rasizm i ksenofobię: art. 256 k.k. – polskie prawo zabrania propagowania faszystowskiego lub innego totalitarnego ustroju państwa oraz nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych lub ze względu na bezwyznaniowość;

- inne nielegalne treści: treści niedotyczące żadnej z powyższych kategorii, ale skierowane przeciwko bezpieczeństwu dzieci, na przykład:
  - propagowanie lub pochwalanie zachowań o charakterze pedofilskim (art. 200b k.k.),
  - uwodzenie dziecka poniżej 15 r.ż. przez internet, tzw. *child grooming* (art. 200a k.k.),
  - zjawisko szantażu na tle seksualnym (art. 197 § 1 kk),
  - patotreści – treści agresywne, przemocowe, promujące niebezpieczne zachowania.

1 Artykuły Kodeksu karnego w brzmieniu niepełnym. Zob. szerzej: Dz. U. z 2024 r. poz. 17 t.j.

Treści przedstawiające seksualne wykorzystywanie dziecka (ang. child sexual abuse material, CSAM)

W zależności od klasyfikacji zgłoszenia oraz lokalizacji serwera, na którym przechowywane są zgłoszone treści, Zespół Dyżurnet.pl zgodnie z procedurą podejmuje następujące działania:

RYSUNEK 2. Schemat obsługi zgłoszeń Dyżurnet.pl

Wszystkie materiały (zdjęcia i filmy) prezentujące seksualne wykorzystywanie dzieci są przekazywane do bazy ICCAM oraz ICSE, aby wspierać identyfikację ofiar i sprawców prowadzoną przez INTERPOL.

Działania wszystkich zespołów reagujących oraz współpracujących z nimi organów ścigania zmierzają do jak najszybszego zidentyfikowania sprawcy oraz pokrzywdzonych wykorzystywaniem seksualnym. Zgłoszenie dokonane przez użytkownika oraz niezwłoczne podjęcie działań przez administratora pozwalają na znaczne ograniczenie dalszego rozpowszechniania materiału przedstawiającego seksualne wykorzystywanie dziecka.

Treści nielegalne oraz treści szkodliwe dla dzieci

W roku 2025 Zespół zaobserwował rosnące zainteresowanie:

- treściami związanymi z szantażem na tle seksualnym,
- wyzwaniami internetowymi zachęcającymi do niebezpiecznych zachowań,
- patotreściami.

Patotreści – przykładem tego typu materiałów są patostreamy, czyli transmisje internetowe prezentujące zachowania patologiczne. Przedstawiają one zachowania niosące demoralizujący przekaz i często mają wulgarny charakter. Najczęściej przedstawiają zachowania agresywne, libacje alkoholowe, podejmowanie niebezpiecznych zachowań, poniżanie innych osób, zażywanie narkotyków.

Innym zjawiskiem zaliczanym do patotreści są utwory muzyczne opisujące i gloryfikujące przemoc – w tym przemoc seksualną, zażywanie narkotyków, nadużywanie alkoholu. Tego typu materiały, poza demoralizującym i szkodliwym przekazem, mogą również łamać przepisy kodeksu karnego.

Ze względu na ich szkodliwość, przede wszystkim dla młodych użytkowników internetu – materiały zawierające patotreści wymagają zdecydowanej reakcji i działań prowadzących do ich usuwania i ograniczania ich promocji. Kluczowym elementem profilaktyki w obszarze cyberbezpieczeństwa jest odpowiednia reakcja platform internetowych oraz edukacja na temat zagrożeń obecnych w sieci – zarówno wśród małoletnich użytkowników oraz ich opiekunów.

Dyżurnet.pl wobec szkodliwych treści popularnych wśród dzieci i młodzieży

Pod koniec 2025 roku Dyżurnet.pl wzmocnił swoje działania w walce z nielegalnymi i szkodliwymi treściami, koncentrując się na szerszym spektrum treści nielegalnych i szkodliwych. Dyżurnet.pl prowadzi monitoring sieci oraz analizę nowych zjawisk i zagrożeń.

Wyniki prowadzonych analiz wraz z rekomendacjami są publikowane na stronie internetowej Zespołu.

20 lat Dyżurnet.pl

Dyżurnet.pl to jedyny w Polsce zespół przyjmujący zgłoszenia dotyczące nielegalnych i szkodliwych treści, które zagrażają bezpieczeństwu dzieci. Przez 20 lat przeanalizował blisko 200 tys. zgłoszeń przekazywanych przez użytkowników internetu oraz instytucje. Były to zarówno treści dokumentujące krzywdę dziecka lub niebezpieczne sytuacje, w których się ono znalazło, jak i materiały szkodliwe dla dzieci w odbiorze. Katalog takich treści stale rozszerza się o nowe zjawiska, zyskujące popularność wśród najmłodszych użytkowników sieci. Reagowanie na nielegalne i szkodliwe treści nie ogranicza się jedynie do kontaktu z moderatorami platform, innymi zespołami reagującymi czy Policją, lecz polega przed wszystkim na analizie trendów oraz budowaniu świadomości społecznej na temat zagrożeń obecnych w cyberprzestrzeni.

Od samego początku Dyżurnet.pl koncentrował się w swoich działaniach na treściach przedstawiających seksualne wykorzystywanie dzieci oraz materiałach pokazujących dzieci w seksualnym kontekście. Pragniemy zwrócić uwagę, że do 2018 roku posługiwaliśmy się terminem „pornografia dziecięca". W celu lepszego oddania istoty zjawiska obecnie upowszechniamy jednak bardziej adekwatne określenie – „materiały przedstawiające seksualne wykorzystywanie dzieci" (CSAM). Obecnie uczestniczymy w grupach roboczych, których celem jest odwzorowanie tego sposobu myślenia w przepisach Kodeksu karnego.

Publikowanie nielegalnych treści, takich jak materiały przedstawiające wykorzystywanie seksualne dzieci, może wynikać z różnych motywacji. Jedną z nich jest chęć wymiany takich materiałów pomiędzy osobami, które uznają je za atrakcyjne i poszukiwane. Z tym zjawiskiem często wiąże się motywacja finansowa – dążenie do osiągnięcia zysku ze sprzedaży trudno dostępnych, postrzeganych jako „ekskluzywne" materiałów. Innymi przyczynami mogą być próby kompromitowania konkretnych osób lub instytucji, a także

działania polegające na przełamywaniu zabezpieczeń systemów i infrastruktury cyfrowej.

Zmiany technologiczne i rozwój internetu spowodowały znaczące przeobrażenia społeczne – prawie każdy posiada urządzenie z aparatem, także dzieci, które z łatwością wykonują zdjęcia. Serwisy społecznościowe, komunikatory, gry umożliwiają bezpośredni kontakt z dziećmi, które spędzają coraz więcej czasu przed ekranem, a tym samym są bardziej narażone na ryzykowne znajomości oraz nieodpowiednie treści. Z drugiej strony nastolatki, szukając swojej tożsamości, testując normy społeczne i budując swoją autonomię, podejmują ryzykowne zachowania, narażając się na potencjalne negatywne konsekwencje.

Takie zmiany wpłynęły również na genezę powstawania materiałów przedstawiających seksualne wykorzystywanie dzieci. I o ile wciąż są dostępne i produkowane materiały, które ukazują wykorzystanie seksualne, które miało miejsce, a sprawca jest sprawcą bezpośrednim, o tyle coraz częściej powstają materiały, które zostały wytworzone przez samych małoletnich. Mogą one powstawać w różnych okolicznościach:

- w wyniku uwodzenia dziecka przez sprawcę kontaktującego się z nim online,
- na skutek szantażu seksualnego,
- w relacjach rówieśniczych, w których materiały intymne zostają później rozpowszechnione bez zgody.

Rozwój sztucznej inteligencji (AI) przyniósł kolejne zagrożenia, umożliwiając wygenerowanie materiałów przedstawiających seksualne wykorzystywanie dzieci na podstawie obrazów prawdziwego dziecka lub wygenerowanej postaci dziecka. Aplikacje nudyfikujące (pozwalające za pomocą technologii „rozebrać" osobę na zdjęciu) są powszechnie dostępne, łatwe w użyciu i popularne wśród młodzieży. Wśród sprawców zauważalna jest tendencja do wymieniania się nie tylko materiałami, ale również sposobami na ich wygenerowanie. Wszystkie powstające materiały mogą mieć postać zdjęcia, filmu, audio, tekstu lub streamingu (transmisji) online, chociaż najczęściej występują zdjęcia i filmy.

Przez 20 lat działania Dyżurnet.pl zmieniły się zarówno narzędzia działania sprawców, jak i metody stosowane przez organy ścigania, w tym podejście do reagowania na produkcję i dystrybucję CSAM. Rozwój narzędzi umożliwiających zaawansowane analizy techniczne, działania dedykowanych zespołów, powołanie międzynarodowych inicjatyw oraz współpraca przedstawicieli branży technologicznej pozwala na podniesienie skuteczności reagowania wobec produkcji i dystrybucji CSAM.

Początkowo działania koncentrowały się przede wszystkim na blokowaniu opublikowanych materiałów. Z czasem zaczęto analizować, kto stoi za publikacją nielegalnych treści. Obecnie możliwe jest również nie tylko docieranie i pociągnie do odpowiedzialności osób dystrybuujących materiały, ale również ich producentów. Co najważniejsze, coraz łatwiejsza jest także identyfikacja dzieci, które potrzebują ratunku. W internecie krążą zarówno materiały powstałe z udziałem osób, które były wówczas dziećmi, a dziś już są dorosłe, jak i nowe treści, będące efektem bieżącego krzywdzenia dziecka. Dlatego kluczowe znaczenie ma rozpoznawanie materiałów już znanych, które są powielane często na masową skalę. Równie istotne jest automatyczne wykrywanie treści, które nie zostały jeszcze przeanalizowane i potwierdzone przez analityka. W tym celu stosowane są narzędzia oparte na sztucznej inteligencji.

W tym kontekście szczególnego znaczenia nabiera precyzyjny język, umożliwiający klasyfikację treści niezależną od regulacji prawnych obowiązujących w poszczególnych krajach. Dlatego INHOPE rozpoczął projekt SCHEMA, w którym istotny udział mieli również eksperci Dyżurnet.pl.

W najbliższej przyszłości Dyżurnet.pl będzie rozwijać narzędzia oparte o AI, wspierające efektywną klasyfikację materiałów, a także brać udział w pracach nad regulacjami krajowymi, które mają na celu usprawnienie całego ekosystemu klasyfikacji treści.

RYSUNEK 3. Źródła pochodzenia materiałów przedstawiających seksualne wykorzystywanie dzieci (CSAM)

Działalność Dyżurnet.pl od początku koncentruje się na reagowaniu na **nielegalne oraz szkodliwe treści dostępne w internecie**, które mogą mieć negatywny wpływ na bezpieczeństwo dzieci i młodzieży. W miarę rozwoju środowiska cyfrowego oraz zmieniających się sposobów korzystania z internetu przez najmłodszych użytkowników zakres analizowanych zjawisk systematycznie się rozszerza.

W ostatnich latach widoczne są również zagrożenia związane ze szkodliwymi treściami, które wpływają na zmiany społeczne i kulturowe. Przykładem są patotreści, czyli materiały prezentujące przemoc, upokorzenie lub inne zachowania naruszające normy społeczne, często rozpowszechniane w celach rozrywkowych. Zjawisko to jest szczególnie niebezpieczne ze względu na swoją popularność wśród młodych odbiorców oraz mechanizmy wzmacniające widoczność tych treści w algorytmach platform społecznościowych, a także powiązania z nadużyciami finansowymi.

Kluczowym elementem skutecznego przeciwdziałania zagrożeniom jest **analiza trendów i mechanizmów rozprzestrzeniania się treści**. Pozwala ona nie tylko na szybsze reagowanie na konkretne zgłoszenia, ale także na identyfikację nowych zjawisk, opracowanie dobrych praktyk dla biznesu oraz opracowywanie działań profilaktycznych. W tym kontekście istotną rolę odgrywa edukacja użytkowników internetu, w szczególności dzieci, młodzieży oraz ich opiekunów. Konieczne są również działania wzmacniające, prowadzone zarówno przez szkoły i instytucje krajowe, jak również przez platformy internetowe, które powinny dostosować swoje produkty do faktycznego wieku ich użytkownika (*safety by design*).

Temat bezpieczeństwa dzieci jest zarówno przedmiotem dyskusji akademickich, jak i branżowych, a wyniki badań i analiz mobilizują do działań wszystkich, którzy mają wpływ na poziom bezpieczeństwa w internecie – w tym w zakresie reagowania na nadużycia, programów profilaktycznych, działań edukacyjnych oraz regulacji prawnych.

W tym kontekście zespoły reagujące, takie jak Dyżurnet.pl, pełnią rolę *trusted flaggers* (zaufanych podmiotów zgłaszających). Nie są tylko specjalistycznym Zespołem, ale stają się formalnym łącznikiem pomiędzy użytkownikami, platformami, a koordynatorem krajowym. Intencją regulacji europejskich jest lepsze zrozumienie potrzeb użytkowników oraz działań platform internetowych, a także usprawnienie procesów związanych z moderacją.

Sprostanie wyzwaniom stojącym przed Dyżurnet.pl wymaga wzmocnienia wewnętrznych struktur, które umożliwią nie tylko podejmowanie obecnych zadań, jak i elastyczne reagowanie na nowe, dynamicznie pojawiające się zagrożenia.

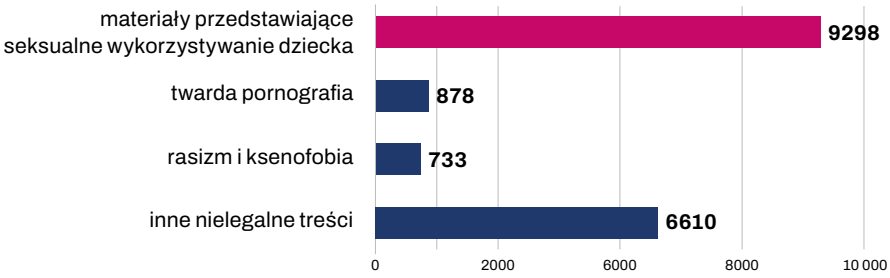
W czasie polskiej prezydencji w Radzie Unii Europejskiej w 2025 roku, realizowanej pod hasłem „Bezpieczeństwo, Europo!", ochrona dzieci i młodzieży w środowisku cyfrowym była obecna wśród tematów związanych z cyberbezpieczeństwem, bezpiecznymi usługami cyfrowymi, przeciwdziałaniem szkodliwym treściom oraz wpływem technologii na zdrowie psychiczne młodych osób.

Dla Dyżurnet.pl szczególne znaczenie miało to, że dyskusja europejska coraz wyraźniej łączy ochronę dzieci online z potrzebą sprawnego reagowania na CSAM, rozwoju narzędzi klasyfikacji treści oraz współpracy między hotline'ami, organami ścigania, instytucjami publicznymi i sektorem technologicznym. Taki kierunek odpowiada doświadczeniom zespołu: od reagowania na pojedyncze zgłoszenia, przez analizę trendów i identyfikację ofiar, po budowanie wspólnego języka oraz narzędzi pozwalających szybciej klasyfikować materiały i ograniczać ich dalsze rozpowszechnianie.

Statystyki Dyżurnet.pl za rok 2025

Zgłoszenia otrzymane przez zespół Dyżurnet.pl

WYKRES 1. Liczba zgłoszeń otrzymanych przez Dyżurnet.pl – podział według rodzaju potencjalnie nielegalnych treści



Po rekordowym pod względem liczby otrzymanych zgłoszeń roku 2024, w roku 2025 odnotowano spadek liczby zgłoszeń w dwóch głównych kategoriach:

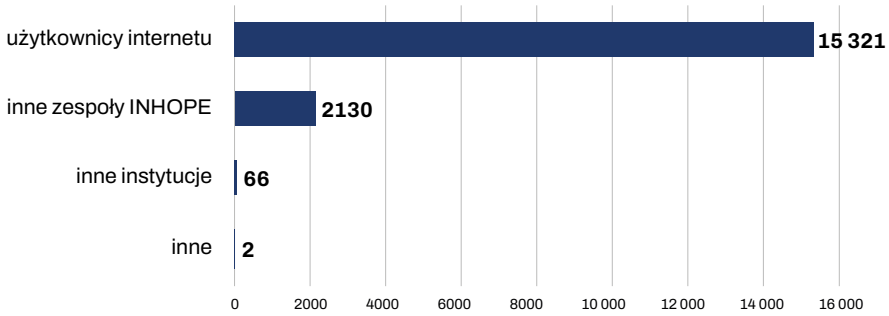
- Liczba **„materiałów potencjalnie przedstawiających seksualne wykorzystywanie dziecka”** była mniejsza o ok. 50% (18 709 w 2024).

- Regularnie spada liczba zgłoszeń w kategorii **„inne nielegalne treści”.** Było ich o ok. 10% mniej niż w roku poprzedzającym (7295 w roku 2024, 9867 w roku 2023).

Nieznacznemu zwiększeniu uległa liczba zgłoszeń w kategorii „twardej pornografii” z 838 w roku 2023 do 878 w roku 2025.

Natomiast liczba zgłoszeń w kategorii „rasizm i ksenofobia” regularnie wzrasta, choć nadal jest najmniej liczna: z 654 w roku 2024 (wówczas wzrost o 100% rok do roku) do 733 w roku 2025.

WYKRES 2. Liczba zgłoszeń otrzymanych przez Dyżurnet.pl – podział według rodzaju podmiotu zgłaszającego

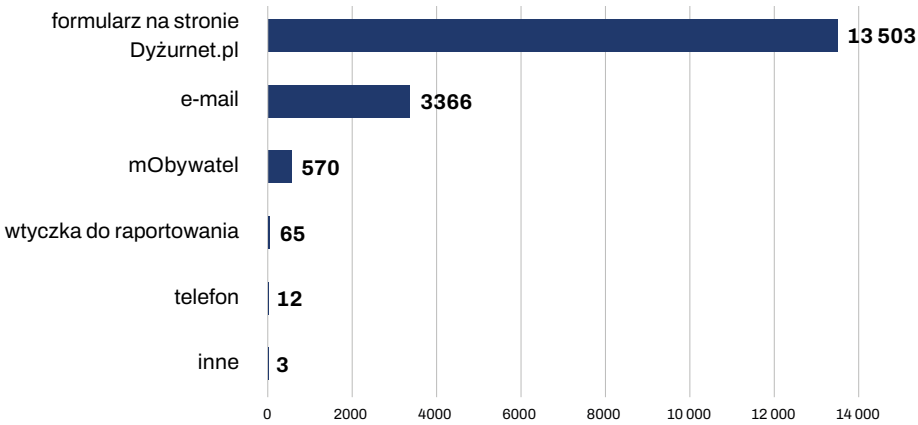


Niezmiennie od lat głównym źródłem powiadomień o potencjalnie nielegalnych treściach są użytkownicy.

Po rekordowym roku 2024 liczba powiadomień otrzymanych od innych zespołów w ramach Stowarzyszenia INHOPE obniżyła się, ale nadal stanowi istotną część zgłoszeń dotyczących treści przedstawiających seksualne wykorzystywanie dzieci – 23%.

Coraz więcej zgłoszeń pochodzi od innych instytucji. Ich liczba wzrosła o 35% w porównaniu z rokiem 2024. Najwięcej spraw Dyżurnet.pl otrzymał od Biura Rzecznika Praw Dziecka interweniującego w kwestiach bezpieczeństwa dzieci w mediach społecznościowych.

WYKRES 3. Liczba zgłoszeń otrzymanych przez Dyżurnet.pl – podział według źródła zawiadomienia



Najczęściej zgłaszający korzystają z formularza na stronie www.dyzurnet.pl, za pośrednictwem którego można anonimowo przekazać powiadomienie o niepokojącej treści, a tym samym uruchomić łańcuch reakcji.

Drugą najczęściej wykorzystywaną formą jest poczta elektroniczna (dyzurnet@dyzurnet.pl), która umożliwia przesłanie załączników dokumentujących nadużycie, m.in. w sprawach seksualnego nagabywania, czy szantażu na tle seksualnym.

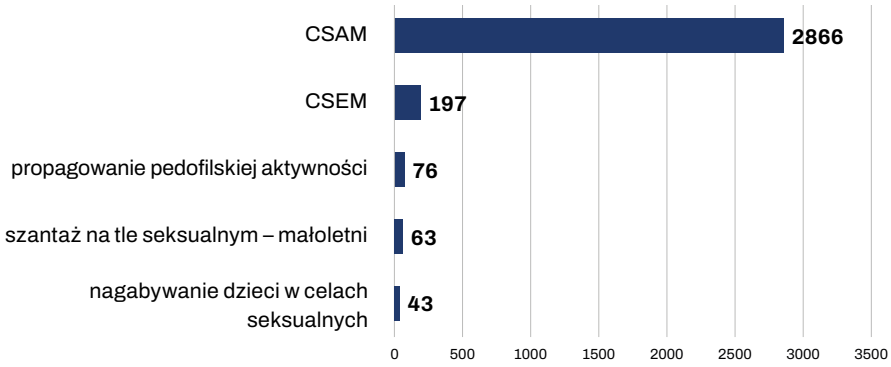
Rośnie liczba zgłoszeń przesłanych poprzez usługę „Bezpiecznie w sieci" w aplikacji mObywatel. Od momentu jej uruchomienia w listopadzie 2024 do zespołu trafiło 570 zgłoszeń. Podobnie jak w przypadku internetowego formularza, zgłaszający może zdecydować, czy pozostawić kontaktowy e-mail umożliwiający informację zwrotną, czy pozostać anonimowy.

Mniej zgłoszeń przekazywanych jest przez wtyczkę do raportowania dla przeglądarek Chrome i Firefox. W związku z uruchomieniem nowego kanału zgłoszeń przez aplikację mObywatel planowane jest wycofanie tego rozwiązania.

Rok 2024 był ostatnim w którym funkcjonowała automatyczna infolinia do przyjmowania zgłoszeń. Usługa ta była najrzadziej wykorzystywana do informowania o potencjalnie nielegalnych treściach, dlatego została wyłączona.

Analizowane incydenty i działania podjęte przez zespół Dyżurnet.pl

WYKRES 4. Klasyfikacja incydentów związanych z wykorzystaniem seksualnym małoletnich



CSAM (*child sexual abuse materials*) – treści przedstawiające seksualne wykorzystywanie dzieci. Zgodnie z polskim prawem nielegalne, definiowane jako treści pornograficzne z udziałem małoletniego (art. 202 § 3, 4, 4a, 4b k.k.).

CSEM (*child sexual exploitation materials*) – treści prezentujące dziecko w kontekście seksualnym, niekwalifikujące się jako CSAM. Obejmuje tzw. „modeling" i „seksualne pozowanie".

Propagowanie pedofilskiej aktywności – publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim; nielegalne wg polskiego prawa (art. 200b k.k.).

Szantaż na tle seksualnym wobec małoletnich – wymuszenie polegające na uzyskaniu od ofiary jej intymnych materiałów, również wygenerowanie takich materiałów przez AI, a następnie żądanie przekazania kolejnych treści lub korzyści materialnych pod groźbą udostępnienia intymnych treści rodzinie, znajomym lub ich szerszego opublikowania. Kwalifikacja prawna może opierać się na art. 190 (groźba karalna), art. 191 (zmuszanie do określonego zachowania) i art. 191a (naruszenie intymności seksualnej). Przestępstwa te **ścigane są na wniosek pokrzywdzonego lub jego opiekuna prawnego.** Mimo że formalnie nie ma ograniczeń w kwestii wieku co do zgłoszenia potencjalnego popełnienia przestępstwa, to w praktyce zgłoszenie powinno być dokonane przez prawnego opiekuna.

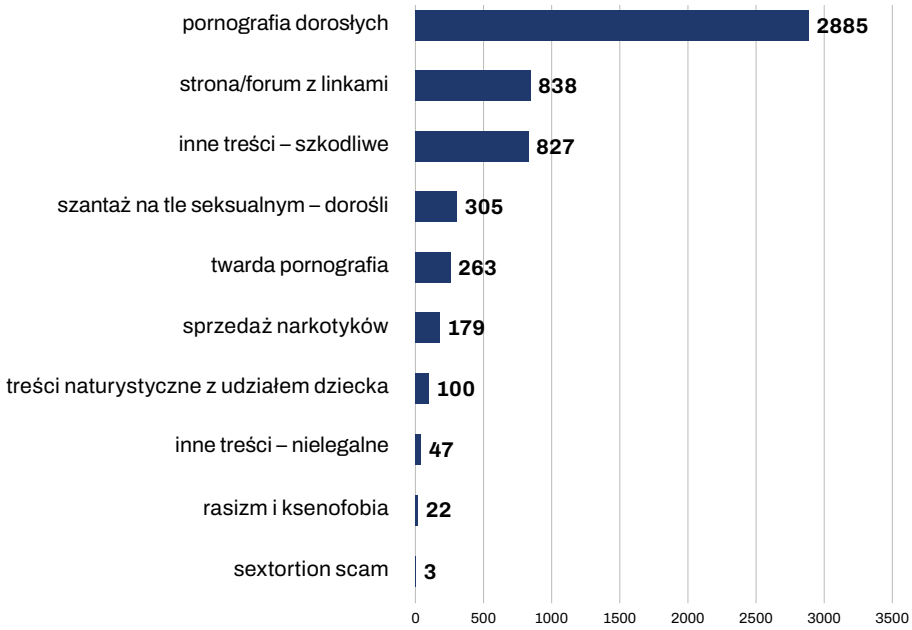
Nagabywanie dzieci w celach seksualnych – nawiązywanie kontaktu z małoletnim poniżej 15 r.ż. celem obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych; zgodnie z polskim prawem nielegalne, art. 200a k.k. (elektroniczna korupcja seksualna małoletniego).

W porównaniu do roku 2024 liczba potwierdzonych incydentów CSAM i CSEM spadła. CSAM blisko o 75% (11 147 w roku 2024), a CSEM o 80%. Wynika to z kilkukrotnych, masowych zgłoszeń dokonanych w 2024 roku przez stowarzyszoną w INHOPE organizację Internet Watch Foundation (więcej na ten temat w Raporcie Dyżurnet.pl za rok 2024). W roku 2025 podobna sytuacja miała miejsce w październiku, kiedy to Dyżurnet.pl otrzymał od zespołu zrzeszonego w INHOPE ponad 1200 zgłoszeń.

Jednak w pozostałych kategoriach nastąpił wzrost: liczba incydentów dotyczących propagowania pedofilskiej aktywności wzrosła o przeszło 160% (z 29 w roku 2024 do 76 w 2025), a liczba incydentów dotyczących nagabywania dzieci w celach seksualnych o blisko 75% (z 26 w roku 2024 do 43 w roku 2025).

Niepokojący jest stały wzrost liczby incydentów dotyczących szantażu na tle seksualnym. W przypadku osób małoletnich, które samodzielnie lub z pomocą rodziców szukały pomocy, liczba takich zdarzeń wzrosła z 17 w roku 2024 do 63 w roku 2025, a więc ponad trzykrotnie.

WYKRES 5. Klasyfikacja incydentów związanych z innymi treściami nielegalnymi i szkodliwymi



Pornografia dorosłych – treści o charakterze pornograficznym z udziałem osób wyglądających na pełnoletnie.

Strona/forum z linkami – strony lub fora internetowe zawierające wyłącznie linki do zewnętrznych zasobów.

Treści naturystyczne z udziałem dziecka – treści prezentujące nagie dzieci bez intencjonalnego seksualnego kontekstu, zazwyczaj treści nudystyczne lub naturystyczne o neutralnym charakterze.

Twarda pornografia – treści pornograficzne z udziałem osób pełnoletnich, zawierające sceny związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem; nielegalne wg polskiego prawa (art. 202 § 3 k.k.).

Szantaż na tle seksualnym wobec dorosłych – wymuszenie polegające na uzyskaniu od ofiary jej intymnych materiałów, ewentualnie wygenerowanie takich materiałów przez AI, a następnie wystosowanie żądania przekazania kolejnych treści lub korzyści materialnych pod groźbą udostępnienia intymnych treści rodzinie, znajomym lub ich szerszego opublikowania.

Sextortion scam – wysyłana masowo korespondencja dotycząca rzekomo pozyskanych materiałów o charakterze seksualnym z udziałem adresata; jedna z form wyłudzeń finansowych skierowana do osób, które padły ofiarą wycieku danych do logowania.

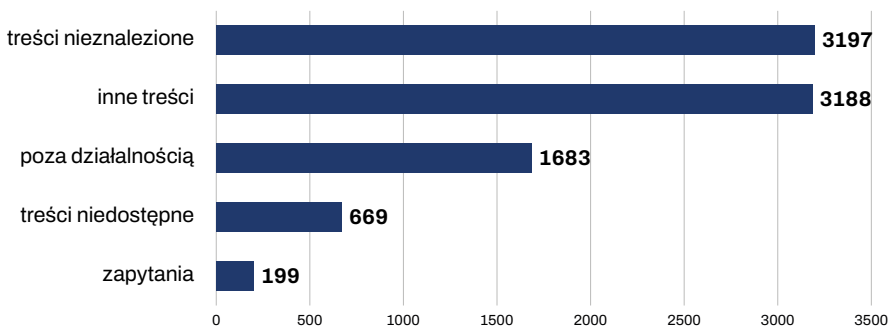
Rasizm i ksenofobia – treści publicznie propagujące totalitarny ustrój państwa, nawołujące do nienawiści oraz znieważające ze względu na przynależność narodową, etniczną, rasową, wyznaniową lub ze względu na bezwyznaniowość; zgodnie z polskim prawem nielegalne (art. 256 oraz 257 k.k.).

WYKRES 6. Klasyfikacja incydentów związanych z treściami szkodliwymi (*n* = 827)

* w tym propagowanie samobójstwa, treści zagrażające życiu lub zdrowiu, treści autodestrukcyjne i promujące zaburzenia odżywiania

Zespół Dyżurnet.pl otrzymał **827 zgłoszeń**, które analitycy oznaczyli jako treści szkodliwe dla osób poniżej 18 r.ż. i przekazali do blokowania w sieci OSE. Poniższy wykres przedstawia rozkład procentowy kategorii, do których zostały przypisane analizowane treści szkodliwe. Materiały, których nie dało się jednoznacznie ocenić, zostały zakwalifikowane do kilku odpowiednich kategorii jednocześnie.

WYKRES 7. Klasyfikacja pozostałych kategorii incydentów



Inne treści – treści spoza wymienionych kategorii, które nie mają charakteru szkodliwego lub nielegalnego.

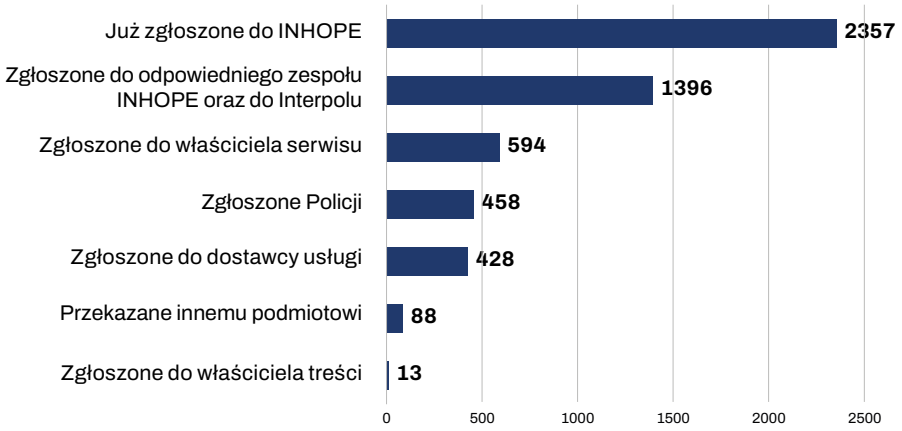
Treści nieznalezione – treści, które w momencie podjęcia analizy przez Dyżurnet.pl nie były już dostępne, najprawdopodobniej zostały już usunięte.

Poza działalnością – sprawy będące naruszeniami prawa, ale wykraczające poza zakres interwencji Dyżurnet.pl: dotyczące danych osobowych (wyłudzenia, udostępnianie bez zgody), wyłudzenia i oszustwa finansowe (w tym fałszywe sklepy internetowe), włamania na konta i kradzież danych, naruszenia praw autorskich, gry hazardowe, dystrybucja farmaceutyków poza obrotem aptecznym, informacje o dostępności zabiegów lub środków przerywania ciąży, publikowanie potencjalnie fałszywych informacji, fałszywe profile instytucji, fałszywe dokumenty.

Treści niedostępne – materiały, do których dostęp jest ograniczony np. zabezpieczone hasłem, pliki do pobrania znajdujące się na serwerach znajdujących się poza Polską, strony zidentyfikowane jako skutecznie maskujące swoją treść.

Zapytania – pytania użytkowników internetu oraz innych instytucji dotyczące nielegalnych i szkodliwych treści publikowanych w sieci.

WYKRES 8. Działania podjęte przez Dyżurnet.pl wobec wszystkich kategorii incydentów



Zgłoszone do odpowiedniego zespołu INHOPE oraz do Interpolu – przesłane poprzez bazę ICCAM lub formularz kontaktowy do zespołów reagujących właściwych dla lokalizacji serwera, zrzeszonych w Stowarzyszeniu INHOPE; treści z kategorii baseline (materiały stanowiące treść nielegalną we wszystkich krajach zrzeszonych w INHOPE) przekazywane są do bazy ICSE (*International Child Sexual Exploitation Database*) w Interpolu.

Zgłoszone do właściciela serwisu – przesłanie zawiadomienia o treściach o charakterze bezprawnym lub szkodliwym dla dzieci i młodzieży. Zgłoszenie z tej kategorii przesłane jest do administratorów lub działu moderacji serwisu internetowego i dotyczy zarówno treści nielegalnych, jak i treści szkodliwych, niezgodnych z regulaminem serwisu.

Zgłoszone do dostawcy usługi – przesłanie zawiadomienia o treściach o charakterze bezprawnym (dotyczących CSAM) do hostingodawcy zlokalizowanego w Polsce, zgodnie z art. 14 ustawy o świadczeniu usług drogą elektroniczną. Stosowane, gdy treść CSAM stanowi usługę strony internetowej utrzymywanej na serwerach hostingodawcy.

Zgłoszone do właściciela treści – zgłoszenie dotyczące treści o szkodliwym charakterze skierowane do autora treści w celu podjęcia decyzji o ich usunięciu lub dodaniu odpowiedniego ostrzeżenia.

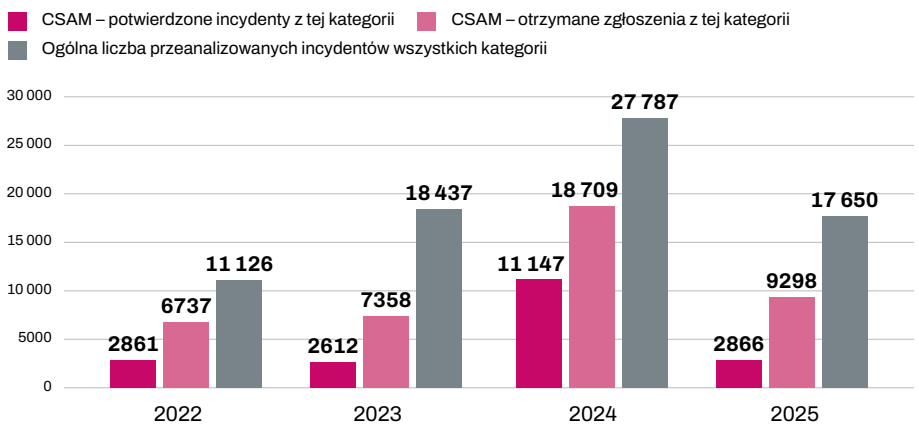
Przekazane innemu podmiotowi – przekazane do współpracujących instytucji zgodnie z zakresem ich działania (głównie CERT Polska w ramach CSIRT NASK oraz Ośrodka Analizy Dezinformacji w ramach NASK – PIB).

Zgłoszone Policji – przekazane do Centralnego Biura Zwalczania Cyberprzestępczości KGP.

Już zgłoszone do INHOPE – informacje o materiałach, które w momencie analizy Dyżurnet.pl były już analizowane przez innych członków Stowarzyszenia.

Analiza treści CSAM

WYKRES 9. Liczba zgłoszeń dotyczących potencjalnych materiałów typu CSAM oraz potwierdzonych incydentów CSAM na tle ogólnej liczby przeanalizowanych incydentów w latach 2022–2025



Po rekordowym roku 2024, dane za rok 2025 osiągnęły podobne wartości do notowanych w latach 2015–2023 i wynosiły odpowiednio w skali roku:

- średnia liczba przeanalizowanych incydentów wszystkich kategorii: 14 000,
- średnia liczba zgłoszeń potencjalnego CSAM: 9257,
- średnia liczba zgłoszeń potwierdzonego CSAM: 2550.

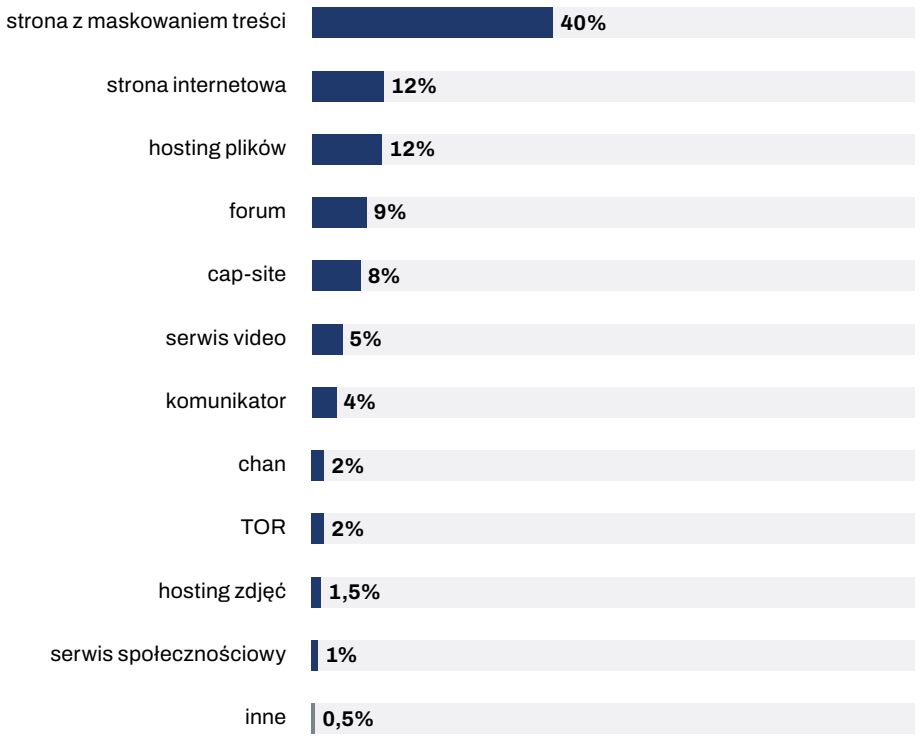
W 2025 roku analitycy Dyżurnet.pl zaobserwowali wyraźny wzrost liczby zgłoszeń dotyczących treści, do których dostęp był w całości bądź częściowo ograniczony. Zjawisko to było bezpośrednio powiązane z rosnącą popularnością zamkniętych platform komunikacyjnych, prywatnych grup oraz serwisów wymagających autoryzacji użytkownika, a także z wykorzystywaniem zabezpieczonych zasobów internetowych, takich jak chmury, repozytoria plików czy usługi dostępne wyłącznie na zaproszenie. Tego typu środowiska znacząco utrudniają szybką weryfikację zgłoszeń i wymagają od analityków podejmowania dodatkowych, często wieloetapowych działań w celu potwierdzenia istnienia nielegalnych treści oraz ich dalszego procedowania.

Jednocześnie zauważono stopniowe odchodzenie od tradycyjnych sposobów rozpowszechniania plików CSAM, polegających na ich bezpośrednim publikowaniu na ogólnodostępnych stronach internetowych lub serwisach hostingowych, gdzie materiały mogły być swobodnie przeglądane i udostępniane przez dowolnego użytkownika internetu. W 2025 roku sprawcy coraz częściej wykorzystywali mechanizmy ograniczające dostęp, takie jak hasła, jednorazowe linki, szyfrowanie przekazu czy zamknięte kanały dystrybucji. Działania te mają na celu zarówno zmniejszenie ryzyka wykrycia, jak i utrudnienie działań podejmowanych przez zespoły monitorujące sieć.

W przypadkach wymagających współpracy międzynarodowej, analitycy Dyżurnet.pl przekazywali zagranicznym partnerom szczegółowe informacje techniczne oraz instrukcje umożliwiające uzyskanie dostępu do zgłaszanych treści – o ile było to niezbędne i zgodne z obowiązującymi procedurami. Równolegle dokonywano zgłoszeń do administratorów oraz właścicieli platform i usług, na których identyfikowano potencjalnie nielegalne materiały, chyba że w danym przypadku podjęto inne uzgodnione działania operacyjne.

Łącznie w 2025 roku podjęto 3848 działań związanych ze zgłaszaniem rozpowszechniania treści CSAM do krajowych organów ścigania oraz zespołów zrzeszonych w INHOPE. Dane te potwierdzają rosnącą skalę i złożoność zjawiska, a także wskazują na konieczność dalszego dostosowywania procedur analitycznych, narzędzi technicznych oraz modelu współpracy międzynarodowej do zmieniających się sposobów dystrybucji nielegalnych treści w środowisku cyfrowym.

WYKRES 10. CSAM analizowany przez Dyżurnet.pl w 2025 roku – lokalizacja w usługach internetowych (*n* = 2866)



Strona internetowa – strona www znajdująca się w otwartych zasobach internetu.

Hosting plików – serwis znajdujący się w otwartych zasobach internetu umożliwiający zamieszczanie, oglądanie i pobieranie przez użytkowników plików różnego rodzaju.

Hosting zdjęć – serwis znajdujący się w otwartych zasobach internetu umożliwiający zamieszczanie, oglądanie i pobieranie przez użytkowników zdjęć oraz grafik.

Serwis wideo – serwis znajdujący się w otwartych zasobach internetu umożliwiający zamieszczanie i oglądanie przez użytkowników plików wideo bez konieczności ich pobierania.

Forum – fora dyskusyjne znajdujące się w otwartych zasobach internetu poświęcone określonej tematyce; mogą zawierać pliki multimedialne.

Serwis społecznościowy – serwis, w ramach którego użytkownicy zakładają własne profile i dzielą się zamieszczanymi przez siebie treściami z innymi użytkownikami.

Strona z maskowaniem treści – strona www znajdująca się w otwartych zasobach internetu, wyświetlająca ukrytą treść po wprowadzeniu odpowiedniego odsyłacza (*http referrer*) lub pliku cookie.

CAP-site (ang. child abuse pyramid sites) – strona www znajdująca się w otwartych zasobach internetu, do której linki umieszczane są w popularnych serwisach społecznościowych. Im więcej dany użytkownik rozpowszechni linków powodując przyrost nowych odwiedzających, tym ma szerszy dostęp do znajdujących się tam płatnych treści CSAM.

TOR (ang. The Onion Router) – zasoby znajdujące się w zanonimizowanej sieci TOR, dostępne wyłącznie za pomocą dedykowanej przeglądarki; większość powyższych usług internetowych może mieć swój odpowiednik w sieci TOR. Adresy zasobów w sieci TOR (tzw. *hidden services*) zawierają pseudodomenę najwyższego poziomu „.onion".

Najczęściej występującą metodą rozpowszechniania CSAM nadal pozostają strony internetowe z maskowaniem treści, choć ich udział spadł z 74% w roku 2024 do 40% w roku 2025. Należy jednak zaznaczyć, że większość tej kategorii stanowią swego rodzaju rozwiązania hybrydowe, łączące funkcje maskujące treść z hostingiem zdjęć oraz plików. Oznacza to, że maskowane są nie tyle całe strony, co pojedyncze pliki CSAM lokowane w serwisach hostingu. Tym należy tłumaczyć istotny spadek kategorii zwykłych, niemaskowanych serwisów hostingowych (z 1560 w roku 2024 do 381 w roku 2025).

Po raz pierwszy widoczny jest znaczny udział tzw. CAP-site, czyli metody wykorzystującej zaangażowanie użytkowników (więcej na ten temat w trendach), choć Dyżurnet.pl obserwował to zjawisko już w poprzednich latach. W roku 2025 wprowadzono oddzielną klasyfikację dla tego typu stron, dzięki czemu trend został uchwycony w danych liczbowych.

Również po raz pierwszy widoczny jest tak istotny udział internetowych komunikatorów w dystrybucji CSAM. Wydawać by się mogło, że sprzyja temu metoda szyfrowania wiadomości *end-to-end*, jednak zdecydowana większość tej kategorii dotyczy komunikatora Telegram, który nie jest szyfrowany.

Popularyzacja komunikatorów i rosnące zagrożenia: przykład Telegram

> **Komunikatory internetowe stają się coraz ważniejszą przestrzenią komunikacji, ale również obszarem rosnących i często ukrytych zagrożeń. Ze względu na zamknięty lub szyfrowany charakter wielu rozmów, dostęp do tych treści jest ograniczony, co utrudnia ich wykrywanie. Do tej pory współpraca z platformami opierała się głównie na ich dobrej woli i była efektem wieloletniego dialogu prowadzonego**

przez Dyżurnet.pl. Wdrażanie przepisów DSA może to zmienić, wprowadzając większą odpowiedzialność platform za reagowanie na nielegalne treści.

Zagrożenia, na jakie narażone są dzieci w środowisku cyfrowym, wykraczają daleko poza klasyczne media społecznościowe. Komunikatory i inne usługi komunikacji online umożliwiają szybkie nawiązywanie kontaktów i wymianę treści, w tym również treści niebezpiecznych, często w przestrzeniach trudnych, a nawet niemożliwych do monitorowania.

Mimo ograniczonych możliwości wpływu regulacyjnego i technologicznego, Dyżurnet.pl podejmuje działania mające na celu współpracę z dostawcami usług cyfrowych, aby minimalizować skalę negatywnych skutków wynikających z korzystania z tych narzędzi przez dzieci i młodzież.

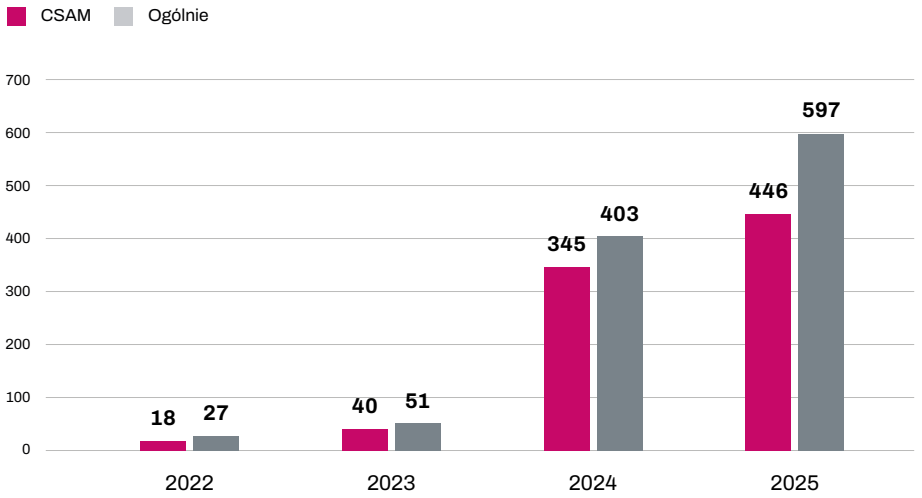
Jednocześnie należy jasno zaznaczyć, że żadne działania podejmowane na poziomie pojedynczej organizacji, ani nawet przez całe sektory, nie są w stanie całkowicie zapobiec zagrożeniom, z jakimi mierzą się dzieci w środowisku cyfrowym. Ograniczenia wiekowe przy zakładaniu kont, czy zmiany regulaminowe nie eliminują zjawiska biernej ekspozycji na szkodliwe treści, które nadal mogą być proponowane przez uzależniające algorytmy czy przekazywane za pośrednictwem szyfrowanych środków komunikacji. Ryzyka związane z cyberprzemocą, groomingiem lub rozpowszechnianiem intymnych materiałów w znacznej mierze przeniosły się do zamkniętych przestrzeni komunikatorów, gdzie są trudniejsze do wykrycia i przeciwdziałania.

Komunikatory, dzięki wygodzie użytkowania i szybkości przekazu, stały się podstawowym narzędziem komunikacji dla milionów osób na całym świecie. W Polsce obserwujemy dynamiczny wzrost ich znaczenia, co przekłada się również na skalę wyzwań związanych z bezpieczeństwem użytkowników. Każdy użytkownik internetu ma do wyboru mnóstwo usług służących do przesłania dowolnych wiadomości, a wśród przesyłanych treści niestety można znaleźć także i te łamiące prawo – w tym materiały przedstawiające seksualne wykorzystanie małoletnich. Jedną z najpopularniejszych w ostatnich latach platform w Polsce jest Telegram, który umożliwia użytkownikom nie tylko wysyłanie prywatnych wiadomości do pojedynczych osób, ale również dołączanie do konwersacji grupowych z nieznajomymi, w tym do grup liczących nawet kilkadziesiąt tysięcy uczestników. Tak duża skala interakcji utrudnia kontrolę nad publikowanymi treściami i znacznie zwiększa ryzyko pojawienia się materiałów nielegalnych – znacznie większe.

Oba sposoby komunikacji są stosowane do zamieszczania zarówno linków do materiałów, jak i bezpośrednio filmów czy zdjęć, często w łatwy sposób przekierowywanych z innych miejsc funkcjonujących w ramach serwisu. Nielegalne treści mogą pojawić się nie tylko na ukrytych, przeznaczonych do tego grupach, ale także i na tych zwykłych, ogólnodostępnych, gdzie

wystarczy chwila nieuwagi administratorów i moderatorów, aby narazić na nie wiele osób. Czasami osoby rozsyłające takie materiały w innych miejscach internetu decydują się również na korzystanie z platformy Telegram i udostępniają w niej swoje indywidualne linki, licząc na to, że pozostaną bezkarne.

WYKRES 11. Liczba zgłoszeń związanych z serwisem Telegram analizowanych przez Dyżurnet.pl w 2025 roku



W ciągu tylko jednego roku Zespół Dyżurnet.pl otrzymał prawie 600 zgłoszeń dotyczących użytkowników i grup udostępniających na tej platformie szkodliwe, najczęściej nielegalne treści. Ponad 440 z nich dotyczyło materiałów przedstawiających seksualne wykorzystywanie dzieci. Pozostałe zgłoszenia odnosiły się do różnego rodzaju zagrożeń, głównie skierowanych wobec dzieci. W porównaniu do roku 2024 roku otrzymaliśmy łącznie prawie 200 zgłoszeń mniej. Warto podkreślić, że to właśnie z serwisu Telegram w ostatnim czasie odnotowaliśmy zdecydowany wzrost zgłoszeń, związany z jego rosnącą popularnością w Polsce.

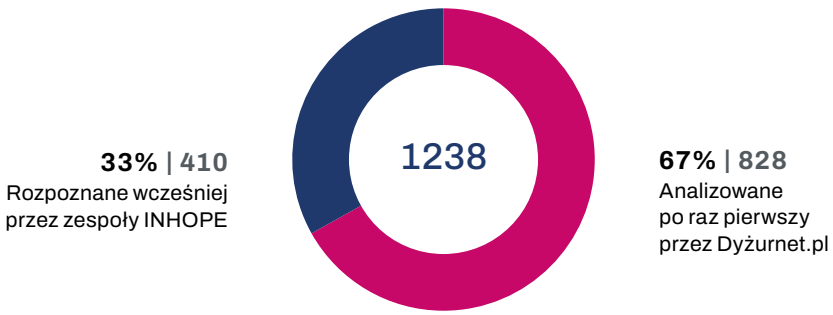
Zauważając coraz większe zainteresowanie platformą Telegram w Polsce, Zespół Dyżurnet.pl podjął rozmowy z jej administratorami, aby znaleźć odpowiednie rozwiązanie na rosnące zagrożenia, skierowane również wobec polskich użytkowników. Dzięki temu wypracowano ścieżkę i metodę komunikacji, w ramach której szkodliwe treści są szybko i skutecznie usuwane z platformy, a dane zabezpieczane dla dalszych celów procesowych. Poza kontaktem z Telegramem, informacje o sytuacji są także przekazywane do partnerskiego zespołu INHOPE, co pozwala na sprawniejsze działania organów ścigania – także poza Polską – niż w przypadku standardowego zgłoszenia do właścicieli serwisu. Współpraca międzynarodowa jest kluczowa, ponieważ materiały często krążą w obiegu globalnym, a sprawcy działają w różnych jurysdykcjach.

Zespół Dyżurnet.pl działa już od 20 lat i nieustannie poszukuje nowych sposobów na zwiększanie skuteczności działań mających na celu ograniczenie liczby nielegalnych treści w internecie. Dostawcy usług, chętnie współpracują w ramach procedury *trusted flagger* (zaufanych podmiotów sygnalizujących), aby przeciwdziałać produkcji i dystrybucji CSAM. Dzięki temu możliwe jest skuteczniejsze reagowanie na udostępniane materiały przedstawiające seksualne wykorzystanie dzieci oraz zwiększenie bezpieczeństwa użytkowników. Taka współpraca podnosi skuteczność działań Dyżurnet.pl, przynosząc jednocześnie korzyści partnerom, którzy również są zainteresowani usuwaniem nielegalnych treści ze swoich platform. Takie pozytywne przykłady dają nam nadzieję, że kolejne firmy będą skłonne do podejmowania współpracy na rzecz wspólnej ochrony użytkowników internetu przed nielegalnymi treściami.

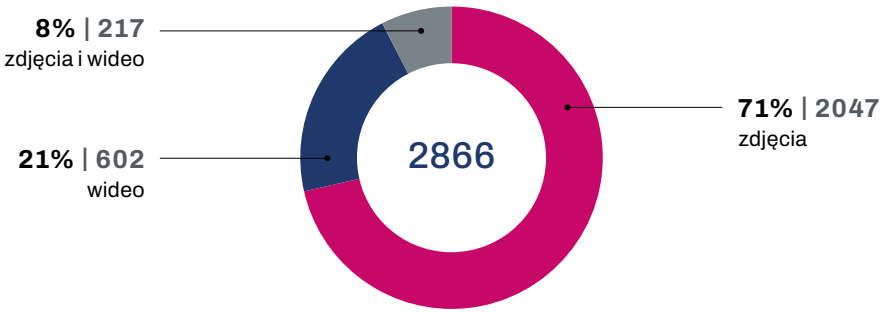
W roku 2025 w trakcie analizy incydentów analitycy Dyżurnet.pl wprowadzili do bazy ICCAM 1238 plików, które zawierały CSAM. Baza ICCAM opiera się na rozpoznawaniu *hash value* (cyfrowego odcisku palca) plików. Dane te uzyskiwane są poprzez zastosowanie funkcji skrótu, pozwalającej na ustalenie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych zbiorów danych. Obrazy i filmy, które zostały zanalizowane i odpowiednio zaklasyfikowane nie są już wyświetlane przy ponownym wprowadzeniu do bazy ICCAM. Dzięki temu rozwiązaniu unika się powielania pracy analityków i poddawania ich czynnikom stresogennym wynikającym z analizy treści.

Spośród tej liczby 67% plików analizowanych było po raz pierwszy. W poprzednich latach liczba ta prezentowała się następująco (2021 – 40%, 2022 – 67%, 2023 – 52%, 2024 – 81%). **Znaczna większość analizowanych treści CSAM to nowo wytworzone materiały.**

WYKRES 12. CSAM analizowany przez Dyżurnet.pl w 2025 roku – liczba plików foto/wideo analizowanych przez Dyżurnet.pl i rozpoznanych już wcześniej przez zespoły INHOPE (*n* = 1238)



WYKRES 13. CSAM analizowany przez Dyżurnet.pl w 2025 roku – rodzaj treści (*n* = 2866)



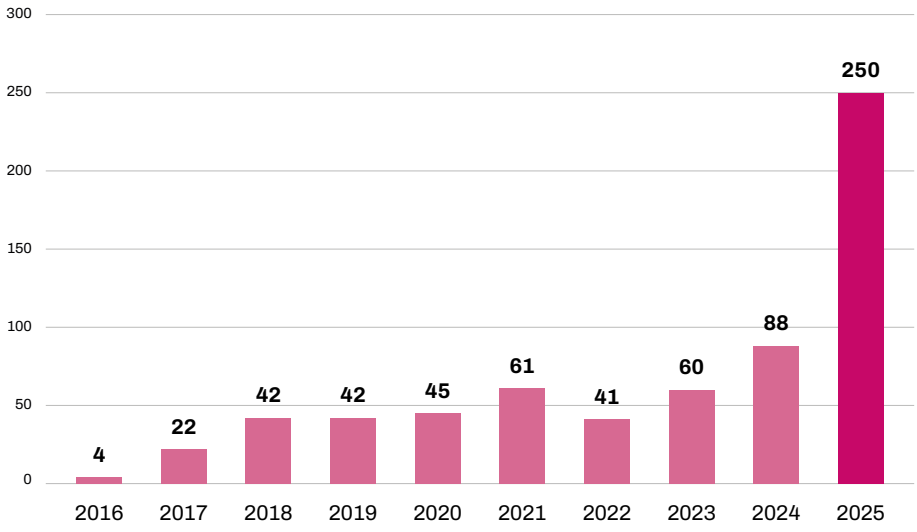
W dotychczasowej analizie rodzaju treści multimedialnych, w roku 2023 treści wideo stanowiły większość (55%). W pozostałych latach dominującą metodą utrwalenia CSAM jest statyczny obraz.

Generatywne treści CSAM

Generatywna sztuczna inteligencja istotnie wpłynęła na wiele aspektów życia. Jej możliwości i łatwość stosowania sprzyjają rozwojowi zagrożeń, obserwowanych przez Dyżurnet.pl. W analizowanych przez ekspertów materiałach widoczne jest użycie sztucznej inteligencji do przerabiania neutralnych treści na materiały o charakterze seksualizującym. Co szczególnie niepokojące, zjawisko to dotyczy nie tylko osób dorosłych, ale również małoletnich.

Rok 2025 przyniósł gwałtowny wzrost liczby materiałów przedstawiających wytworzone lub przetworzone treści prezentujące seksualne wykorzystanie małoletniego. Wynosi on prawie 300%. W poprzednich latach obserwowany był udział wygenerowanych komputerowo, realistycznych materiałów jednak dających się odróżnić od realnych. Obecna technologia AI praktycznie uniemożliwia ocenę czy dany obraz jest realny czy został wytworzony. W związku z tym liczba takich materiałów może być jeszcze wyższa.

WYKRES 14. Generowany CSAM analizowany przez Dyżurnet.pl w latach 2016–2025



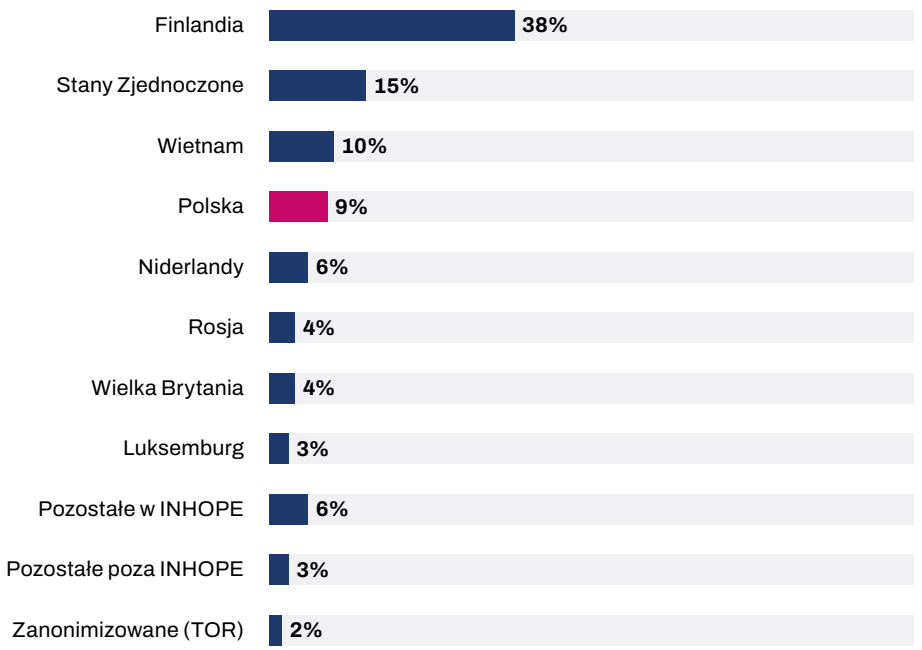
Problem ten istotny ze względu na następujące kwestie:

- **Niedostosowanie obecnych zapisów prawnych.** Niektóre państwa nie penalizują takich materiałów. Polski Kodeks karny zwraca uwagę na treści prezentujące „wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej". Określenie to zawęża spektrum penalizowanych treści, które w pozostałych paragrafach tego artykułu określane są jako „pornograficzne". W praktyce oznacza to, że wygenerowane obrazy nagich osób w tzw. seksualnym pozowaniu mogą być traktowane jako legalne.

- **Problem dla organów ścigania.** Kryterium *baseline* używane przez INTERPOL (patrz Wykres 18) dotyczy wyłącznie realnych dzieci, które należy jak najszybciej zidentyfikować, oddzielić od sprawcy seksualnych przestępstw i zapewnić im bezpośrednią pomoc. W przypadku treści generowanych przez AI może to wpływać na efektywność podejmowanych działań i nieskuteczne angażowanie zasobów.

- Materiały przetworzone czy wytworzone na podstawie innych zdjęć i filmów również są formą przemocy. Mogą również prowadzić do normalizacji zachowań seksualnych wobec dzieci oraz służyć manipulacji podczas nagabywania seksualnego. Ze względu na drastyczność materiały są takim samym obciążeniem dla analityków podczas ekspozycji na treści.

WYKRES 15. CSAM analizowany przez Dyżurnet.pl – lokalizacja serwerów w odniesieniu do adresów URL (*n* = 2866)



Lokalizacja serwera z treścią CSAM jest kluczowa dla skutecznej reakcji. Zespół Dyżurnet.pl wyróżnia dwa rodzaje lokalizacji:

- w odniesieniu do adresu URL
- w odniesieniu do plików foto/wideo

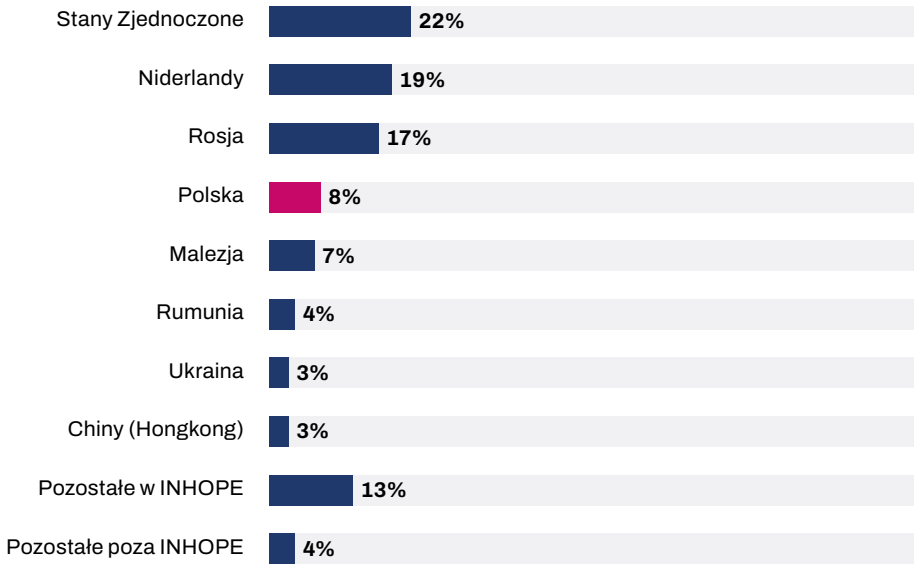
Przykładowo strona przedstawiająca treści CSAM http://abc.com znajduje się na serwerze zlokalizowanym w USA. Lokalizację tego typu pokazuje Wykres 15. Jednak nielegalne pliki foto lub wideo wyświetlane przez tę stronę znajdują się na serwerach innych państw, np. Holandii lub USA. Lokalizację plików CSAM pokazuje Wykres 16.

Polska niestety nadal plasuje się wysoko w zestawieniu lokalizacji serwerów z CSAM. Zdecydowana większość spraw odnotowanych przez analityków dotyczy serwisów hostingowych, na które użytkownicy mogą przesyłać pliki.

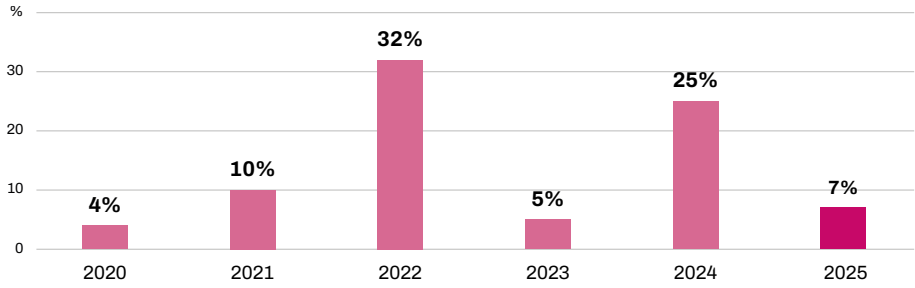
Dyżurnet.pl rekomenduje wprowadzenie automatycznych systemów rozwiązań weryfikujących *hash value* przesyłanych plików, co pozwoli na identyfikację i eliminację tych zawierających rozpoznany CSAM.

Więcej informacji można uzyskać kontaktując się z zespołem Dyżurnet.pl info@dyzurnet.pl.

WYKRES 16. CSAM analizowany przez Dyżurnet.pl – lokalizacja serwerów w odniesieniu do plików foto/wideo (*n* = 828)

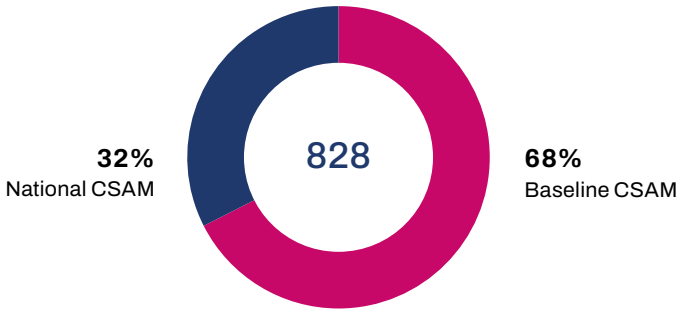


WYKRES 17. CSAM analizowany przez Dyżurnet.pl w latach 2020–2025 – odsetek lokalizacji plików foto/wideo poza zasięgiem INHOPE w latach 2020–2025



W 2025 roku zaobserwowano powrót do relatywnie niewielkiego udziału plików zawierających treści CSAM publikowanych poza zasięgiem działalności zespołów reagujących zrzeszonych w Stowarzyszeniu INHOPE. Od 2022 roku w INHOPE obowiązuje procedura pozwalająca określonym zespołom stowarzyszenia interweniować bezpośrednio u zagranicznego hostingodawcy w celu usunięcia treści CSAM.

WYKRES 18. CSAM analizowany przez Dyżurnet.pl w 2025 roku – podział ze względu na kategorię treści (*n* = 828)



Baseline CSAM (kryteria nielegalności we wszystkich państwach współpracujących z Interpolem):

- Obraz prawdziwego, realnego dziecka. Obrazy wygenerowane komputerowo, narysowane lub w jakikolwiek inny sposób wytworzone czy przetworzone nie są uwzględniane.
- Dzieci przedstawione w sytuacjach seksualnego wykorzystania są w okresie przedpokwitaniowym (nie osiągnęły 13 r.ż.).
- Przedstawienie sytuacji seksualnego kontaktu lub zogniskowanie na rejonie genitalnym lub analnym dziecka.

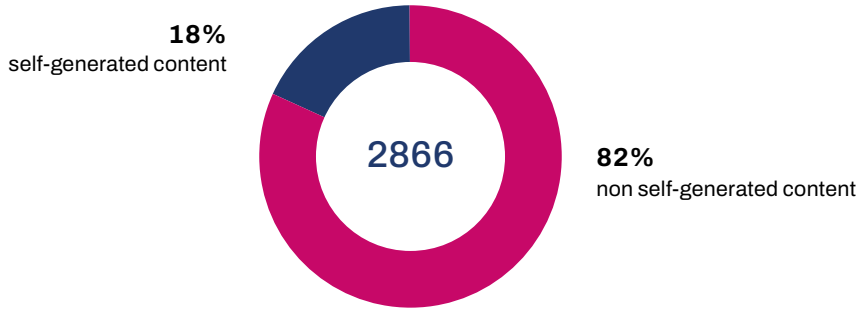
National CSAM

- Treści o charakterze pornograficznym z udziałem osób małoletnich powyżej 13 roku życia (te z osobami młodszymi klasyfikowane są jako *baseline* CSAM).

- Treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej.

W ostatnich latach odsetek najbardziej drastycznych treści kategorii *baseline* jest w miarę stabilny i stanowi większość analizowanych materiałów.

WYKRES 19. CSAM analizowany przez Dyżurnet.pl w 2025 roku – udział treści o charakterze pornograficznym wytworzonych przez ofiary (*self-generated sexual content*) (*n* = 2866)



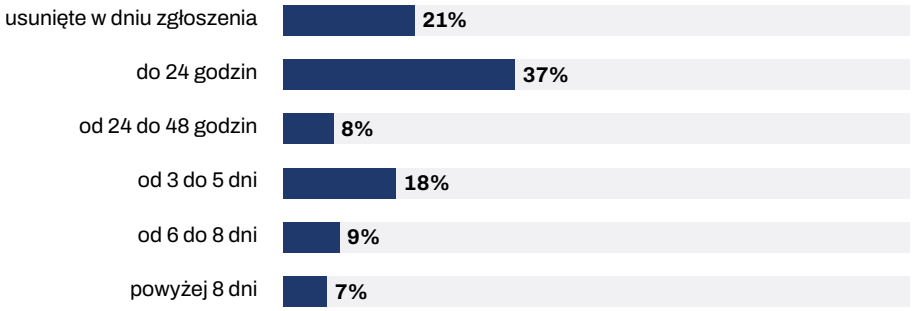
Self-generated sexual content – materiał foto/wideo wytworzony samodzielnie przez osobę małoletnią, uzyskany za jej zgodą lub bez jej zgody, przedstawiający ją w trakcie czynności o charakterze seksualnym. Należy pamiętać, że **samodzielna produkcja materiałów nie oznacza rozumienia przez dzieci całego kontekstu sytuacji oraz nie stanowi o tym, że materiały są wytworzone dobrowolnie**. Więcej na ten temat znajduje się w naszej publikacji „Ryzykowne zachowania seksualne i seksualizacja młodych użytkowników internetu. Zarys problematyki”[2].

W roku 2025 udział materiałów wytworzonych samodzielnie przez małoletnich wyniósł 18%, co stanowi względnie stabilny poziom w porównaniu z poprzednimi latami. Warto zaznaczyć, że pojedyncze incydenty zazwyczaj dotyczą forów, na których umieszczane są tysiące tego typu materiałów, wytwarzanych zarówno przez nastolatki, jak i dzieci w wieku wczesnoszkolnym.

2 Dyżurnet.pl. (2020). *Ryzykowne zachowania seksualne i seksualizacja młodych użytkowników internetu. Zarys problematyki. NASK – PIB*. https://dyzurnet.pl/uploads/2020/04/Ryzykowne_zachowania_na_www.pdf

Dyżurnet.pl rekomenduje zachowanie szczególnej ostrożności w przypadku transmisji online prowadzanych przez dzieci. Rozmówca może zmanipulować lub zastraszyć dziecko i skłonić je do odkrycia części intymnych lub zachowań seksualnych, nagrać transmisję bez zgody. Tak pozyskane materiały mogą zostać opublikowane lub wykorzystane do szantażu w celu zdobycia kolejnych materiałów lub pozyskania korzyści finansowych.

WYKRES 20. Czas publicznej dostępności CSAM/CSEM zlokalizowanych w Polsce i zgłoszonych do Dyżurnet.pl przez inne zespoły INHOPE w 2025 roku (*n* = 321)



W 66% przypadków treści CSAM były blokowane w ciągu 48 godzin od zgłoszenia Dyżurnet.pl. W pozostałych 34% blokada następowała później, w tym 8% treści pozostawało dostępnych ponad 8 dni. Wskazuje to na potrzebę wdrożenia w Polsce formalnej procedury Notice & Action przewidzianej w DSA.

Działania podejmowane przez Dyżurnet.pl wobec nielegalnych i szkodliwych treści

Od 2015 roku zespoły reagujące zrzeszone w INHOPE korzystają ze zintegrowanej bazy wymiany informacji dotyczących CSAM. Baza ICCAM pozwala na klasyfikację plików foto i wideo zamieszczonych pod określonym adresem URL. Materiały klasyfikowane są ze względu na cechy ofiary, takie jak płeć oraz przybliżony wiek. Najistotniejsze jest rozpoznanie materiałów stanowiących treść nielegalną we wszystkich krajach zrzeszonych w INHOPE (*baseline*). Informacja o najbardziej drastycznych materiałach przekazywana jest bezpośrednio do bazy ICSE (*International Child Sexual Exploitation database*), co umożliwia podjęcie działań w celu identyfikacji zarówno ofiar, jaki i sprawców.

Warto zauważyć, że materiały przedstawiające seksualne wykorzystywanie dzieci, publikowane są w otwartym internecie w taki sposób, aby nie natrafiły na nie osoby przypadkowe. Dlatego też ważna jest współpraca międzynarodowa na poziomie analitycznym – wymiana informacji o plikach, o miejscu ich publikacji, a także adresach URL.

W 428 przypadkach zespół Dyżurnet.pl kontaktował się bezpośrednio z dostawcami usług w celu poinformowania o treściach bezprawnych (dotyczących CSAM) znajdujących się na ich serwerach. Po powiadomieniu publiczny dostęp do treści jest blokowany, a odpowiednie dane zostają zabezpieczone na potrzeby działań organów ścigania. Informacje są również przekazywane policji.

W przypadku treści szkodliwych dla dzieci i młodzieży Dyżurnet.pl przekazuje informacje o nadużyciach właścicielom serwisu. Działania takie są podejmowane zarówno wobec stron polskich, jak i zagranicznych – w 2025 roku dotyczyło to 594 incydentów.

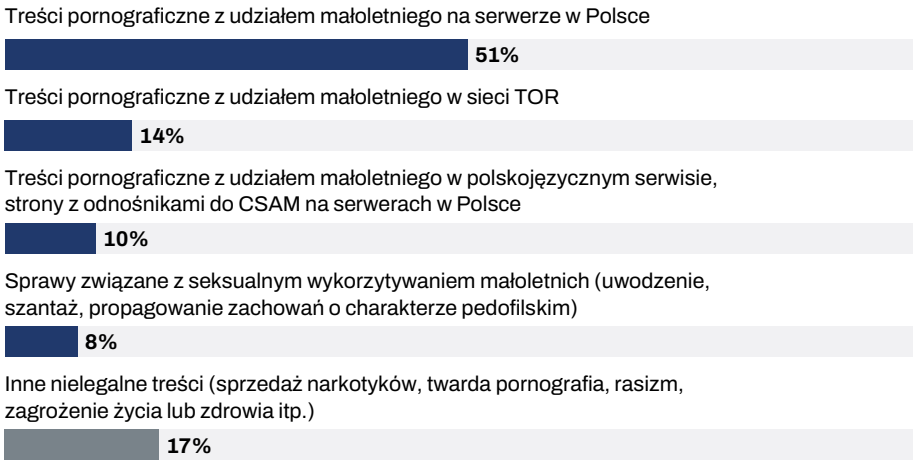
Ze względu na zakres wykraczający poza ramy działalności Dyżurnet.pl, 88 spraw zostało przekazanych innym podmiotom – m.in. działającym w ramach NASK – PIB zespołom CERT Polska oraz Ośrodkowi Analizy Dezinformacji.

458 incydentów zgłoszono do Centralnego Biura Zwalczania Cyberprzestępczości Komendy Głównej Policji. Dotyczyły one przede wszystkim seksualnych nadużyć wobec dzieci.

Zgłoszenia związane z CSAM stanowiły 75% przekazanych incydentów (na polskich serwerach – 231, w polskojęzycznych serwisach – 47, w sieci TOR – 65). 38 spraw związanych było z nagabywaniem dzieci poniżej 15 r.ż w celach seksualnych, szantażem seksualnym wobec małoletnich oraz propagowaniem zachowań o charakterze pedofilskim.

77 spraw (17%) zgłoszonych do Policji obejmowało inne nielegalne treści, takie jak sprzedaż narkotyków, twardą pornografię, rasizm, zagrożenie życia lub zdrowia itp.

WYKRES 21. Kategorie incydentów przekazanych przez Dyżurnet.pl do Centralnego Biura Zwalczania Cyberprzestępczości w 2025 roku



Szanse i osiągnięcia

Terminologia, która pomaga chronić dzieci: CSAEM, OCSAE

Terminologia stosowana w opisie zagrożeń wobec małoletnich w środowisku cyfrowym wpływa na skuteczność rozpoznawania zjawisk, szybkość reagowania na nie, a także współpracę międzyinstytucjonalną. Może też stanowić element systemu ochrony dzieci, chociażby tylko dlatego, że nie naraża ich na wtórną wiktymizację czy traumatyzację. W tym kontekście coraz większe znaczenie zyskują próby porządkowania i ujednolicania pojęć, takie jak Universal Classification Schema (UCS) – międzynarodowy system klasyfikacji opracowany przez sieć INHOPE i partnerów, który pomaga w spójnym opisywaniu i klasyfikowaniu materiałów przedstawiających seksualne wykorzystywanie dzieci. W tej części Raportu omawiamy rolę definicji, ich ewolucję, a także znaczenie podejścia skoncentrowanego na osobie pokrzywdzonej (ang. victim-centered approach).

Precyzyjny język używany do opisu zjawisk zachodzących w środowisku cyfrowym stanowi integralny element skutecznej ochrony małoletnich. Terminologia stanowi odzwierciedlenie obowiązujących dziś narzędzi poznawczych, aktualnego stanu wiedzy, uwarunkowań kulturowych, praktyk instytucjonalnych, ram prawnych, a także indywidualnej i społecznej wrażliwości[3,4]. Jej spójność i jednoznaczność sprzyjają właściwej kwalifikacji zjawisk (np. CSAEM jako forma cyberprzestępstwa), poprawiają komunikację (np. między dzieckiem a instytucjami państwowymi), a także – co może nie jest już tak oczywiste – ułatwiają użycie technologii wspierających analizę materiałów przedstawiających seksualne wykorzystywanie i eksploatację dzieci (np. modele AI do preklasyfikacji CSAEM).

3 ECPAT International. (2025), *The Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, wyd. 2, s. 1, [dalej: Wytyczne]

4 INHOPE, What is... Terminology and Technology [źródło: https://inhope.org/media/pages/articles/inhope-guidelines-on-advocacy-initiating-legislative-changes/3de-4555bd2-1766155091/inhope-guidelines-on-advocacy-initiating-legislative-changes.pdf]

Podstawowe pojęcia i skróty: potrzeba jednoznaczności

W dyskursie międzynarodowym stosuje się szereg akronimów i definicji opisujących treści oraz aktywności naruszające dobro małoletnich. CSAEM – ang. *child sexsual abuse & exploitation materials*, tj. **materiały/treści przedstawiające seksualne wykorzystywanie dzieci** oraz OCSAE – ang. *online child sexsual abuse & exploitation*, tj. **seksualne wykorzystywanie dzieci w Internecie** (dosłownie: online), to dwa podstawowe terminy związane z międzynarodową ochroną dzieci przed cyberprzestępczością na tle seksualnym.

RYSUNEK 4. Wizualizacja pojęć CSAE, CSAEM, OCSAE. Źródło: opracowanie własne

Termin **CSAM** (*child sexual abuse materials*) odnosi się do materiałów przedstawiających seksualne wykorzystywanie dzieci jest powszechnie używany i bardziej adekwatny niż wciąż stosowany termin „pornografia dziecięca" lub prawnicze „treści pornograficzne z udziałem osób małoletnich". Pornografia odnosi się do osób dorosłych, które dobrowolnie uczestniczą w czynnościach seksualnych (np. w celach zarobkowych lub rozrywkowych) oraz mają możliwość wycofania się z sytuacji. W przypadku dzieci nie może być mowy o dobrowolności – każdy taki materiał jest **dowodem przestępstwa**, na podstawie przepisów karnych we wszystkich krajach współpracujących z Interpolem.

Termin **CSEM** (*child sexual exploitation materials*) odnosi się również do materiałów uprzedmiatawiających dziecko jako obiekt seksualny, które jednak pokazują dziecko w seksualnym kontekście. W tej kategorii mieszczą się m.in. *child modeling* czy seksualne pozowanie[5,6]. W odróżnieniu od CSAM, taki materiał jest **dowodem przestępstwa**, na podstawie przepisów karnych w wybranych krajach.

Termin **OCSAE** (*online child sexual abuse and exploitation*) stanowi ogólną kategorię aktywności sprawców przemocy seksualnej wymierzonej przeciwko

5 *Wytyczne*, s. 63–66.

6 Dyżurnet.pl. (2016). *Treści pornograficzne z udziałem dzieci. Zarys problematyki*, s. 10.

dzieciom w cyberprzestrzeni, w której dominującą rolę odgrywają technologie teleinformatyczne; obejmuje on m.in. grooming, nakłanianie małoletnich do podejmowania czynności seksualnych w środowisku online (np. przed kamerką), udostępnianie i monetyzacja treści CSAEM, szantażowanie dziecka, a także produkcję treści CSAEM z użyciem sztucznej inteligencji, np. na podstawie neutralnych zdjęć pozyskiwanych w następstwie tzw. *sharentingu*[7,8,9].

Ewolucja języka: od ujęć historycznych do podejścia skoncentrowanego na pokrzywdzonym

Analizując historię polskiego i międzynarodowego prawa, widzimy jak zmienia się język opisu przemocy wobec dzieci. Jeszcze w 1969 roku polski Kodeks karny mówił o „czynach lubieżnych", co dziś odbierane jest jako archaiczne i niedostatecznie oddające traumę dziecka. Nawet nowsze dokumenty, jak polskie tłumaczenie Dyrektywy 2011/92/UE, używają sformułowań takich jak „niegodziwego traktowanie w celach seksualnych i wykorzystywanie seksualne dzieci" czy „pornografia dziecięca".

Obecnie standardem staje się **podejście skoncentrowane na osobie pokrzywdzonej** (ang. *victim-centered approach*). Zgodnie z **Wytycznymi**, należy unikać terminów stygmatyzujących, takich jak „dziecięca prostytucja" na rzecz „dziecka wyzyskiwanego w prostytucji". Język powinien bowiem jednoznacznie i precyzyjnie wskazywać jednokierunkowy (sprawca → dziecko), przemocowy charakter tych działań.

Język opisujący związany z szeroko pojętą ochroną małoletnich ulegał zmianom wraz z rozwojem wiedzy, standardów etycznych i regulacji prawnych. Współczesne podejście kładzie nacisk na:

- **neutralność i precyzję** sformułowań,
- **jednoznaczne wskazanie relacji sprawczej** (działanie dorosłego wobec małoletniego),
- **minimalizowanie ryzyka stygmatyzacji** poprzez odpowiedni dobór słownictwa,
- **kompatybilność między systemami prawnymi i technologicznymi**.

7 Dyżurnet.pl. (2024). Raport, s. 17.

8 Ali, S., Paash, A.S. (2021). A systematic review of the technology enabled child sexual abuse (OCSA) & it's impacts, *Journal of Legal, Ethical and Regulatory Issues*, *25*(S5), 1–18.

9 Brown, R. (2023). *Eliminating Online Child Sexual Abuse Material*.

Funkcje języka w reagowaniu na zagrożenia wobec małoletnich (w środowisku cyfrowym)

Raporty Dyżurnet.pl (dostępne do pobrania na naszej stronie https://dyzurnet.pl/publikacje) stanowią doskonały przykład zmian zachodzących w identyfikowaniu, reagowaniu, ale też opisywaniu zjawisk związanych z seksualnym krzywdzeniem małoletnich. Stosowany na samym początku termin „pornografia dziecięca" został słusznie zastąpiony w publikacjach przez oddający istotę „materiały przedstawiające seksualne wykorzystywanie dziecka", przy czym należy zauważyć, że art. 202 Kodeksu karnego odnosi się do „treści pornograficznych z udziałem osób małoletnich". Aktualnie trwają prace legislacyjne nad zmianą stosowanej terminologii.

Precyzyjne nazewnictwo – co podkreślamy w naszych *Raportach* [10,11,12] – służy kilku celom:

1. **Podejście skoncentrowane na pokrzywdzonym** – język powinien uwzględniać perspektywę osoby małoletniej, podkreślając charakter naruszenia jej dóbr osobistych oraz skutki psychologiczne:

   CSAM (*child sexual abuse materials*) – to termin określający materiały przedstawiające seksualne wykorzystywanie dziecka. Jest on bardziej adekwatny od terminu „pornografia dziecięca", ponieważ kładzie nacisk na fakt wykorzystania dziecka w świecie realnym. Zamieszczenie w internecie CSAM może być tylko jednym z etapów przestępczego działania – począwszy od uwiedzenia dziecka, wykorzystania seksualnego i udokumentowania tego aktu, a następnie udostępniania i rozpowszechniania takiego materiału.

2. **Wsparcie postępowania dowodowego** – jednoznaczne opisy treści, relacji i zdarzeń sprzyjają właściwej interpretacji materiałów, a także użyciu ich w dalszych czynnościach operacyjnych i procesowych:

   Każde zdjęcie czy film wideo to w rzeczywistości dowód przestępstwa popełnionego wobec dziecka. Za każdym zdjęciem stoi ofiara i sprawca.

3. **Łączenie systemów i technologii** – spójny (meta)język umożliwia automatyczną translację między schematami klasyfikacji, ułatwiając współpracę instytucji publicznych i podmiotów technologicznych:

10 Dyżurnet.pl. (2014). *Raport*, s. 10.

11 Dyżurnet.pl. (2011). *Raport*, s. 3.

12 Dyżurnet.pl. (2023). *Raport*, s. 58.

Celem SCHEMA, międzynarodowego projektu Global Standard realizowanego przez INHOPE i finansowanego przez Global Partnership to End Violence against Children jest stworzenie **wspólnej ontologii dla istniejących na świecie systemów kategoryzacji treści CSAM**, która umożliwi automatyczną translację pomiędzy takimi systemami funkcjonującymi dzisiaj w różnych krajach i instytucjach. **Wspólny język opisujący cechy charakterystyczne w poszczególnych kategoriach treści pozwoli wszystkim zaangażowanym instytucjom i podmiotom na efektywną wymianę danych bez konieczności ich ponownej analizy.** Umożliwi również szybkie podjęcie decyzji o potencjalnej nielegalności każdej skategoryzowanej treści. Z systemu będą mogli korzystać zarówno analitycy *hotline*, funkcjonariusze policji, jak i specjaliści branży technologicznej.

Wspólna ontologia pojęć i klasyfikacji (Universal Classification Schema)[13]

Opracowanie i wdrożenie uniwersalnego schematu klasyfikacji CSAM pozwala na:

- **szybszą wymianę danych** między krajowymi zespołami *hotline*, organami ścigania i podmiotami technologicznymi (np. ISP/ICP);
- **automatyczne mapowanie kategorii** pomiędzy różnymi systemami prawnymi;
- **wzbogacenie opisu materiałów** o takie cechy, jak przedmiot, kontekst i cechy identyfikacyjne, co wspiera działania operacyjne i procesowe.

Ponadto taki uniwersalny i wzbogacony system klasyfikacji – odpowiednio wdrożony i zautomatyzowany – pozwala uzyskać więcej informacji na temat materiałów CSAM, które mogą być użyte na potrzeby szeroko pojętego procesu karnego i czynności operacyjnych, w tym identyfikacji grupowej potencjalnych pokrzywdzonych (ang. VID, *victim identification*). Minimalizuje wtórną wiktymizację oraz zmniejsza ekspozycję na treści CSAM. Zdjęcia i filmy opisane zgodnie z *Universal Classification Schema*, ujawnione podczas

13 https://universalclassificationschema.org/

przeszukania w ramach triażu[14], mogą m.in. dostarczyć informacji o charakterze treści CSAM, grupie wiekowej czy płci osób pokrzywdzonych. Dzięki tym informacjom bezpośrednio po zakończeniu przeszukania (a niejednokrotnie już w jego trakcie) można:

- Podjąć czynności zmierzające do identyfikacji potencjalnych pokrzywdzonych w najbliższym otoczeniu sprawcy (np. w domu, sąsiedztwie lub miejscu pracy) i udzielenia im niezbędnej pomocy.

- Wykonać wstępne profilowanie sprawcy (zarówno w zakresie występowania parafilii, typu użytkownika CSAM, a także ewentualnej roli w grupie przestępczej), co pozwoli na bardzo wstępnym etapie rozróżnić: sprawcę kontaktowego, od tzw. kolekcjonera treści CSAM, czy członka zorganizowanej grupy przestępczej odpowiedzialnego za monetyzację CSAM. W dużym uproszczeniu: pierwszy posiada materiały z zapisem aktywności seksualnych z dzieckiem/dziećmi, w którym sam bierze udział; drugi kataloguje i opisuje na nośnikach cyfrowych różnorodne treści, które stanowią dla niego tzw. atraktor; ostatni – zamiast znacznych zbiorów CSAM (chociaż nie należy ich wykluczyć), może posiadać zapis udokumentowanych transakcji związanych z wykorzystywanym dzieckiem, bazę klientów, czy np. fizyczne portfele kryptowalut.

- Efektywniej zaplanować dalsze czynności (np. wniosek o areszt, powołanie biegłych, podjęcie międzynarodowej współpracy z organami ścigania lub podmiotami zaangażowanymi w zwalczanie CSAM).

Beneficjentami efektywnego, planowego i nowoczesnego użycia języka, mogą być przede wszystkim dzieci, ale też organy ścigania i wymiar sprawiedliwości. Jednolita i precyzyjna terminologia jest jednym z podstawowych elementów skutecznej ochrony małoletnich w środowisku cyfrowym. Wspiera współpracę między instytucjami, poprawia jakość przetwarzania, analizy, klasyfikacji i kategoryzacji treści CSAM. Rekomendowane jest wdrażanie wspólnych schematów pojęciowych oraz jasnych, precyzyjnych definicji, tak na poziomie technologii, czy prawa, jak i metodologii (np. algorytmów czynności procesowych, operacyjnych).

14 Triaż – stosowany m.in. w informatyce śledczej proces szybkiej identyfikacji dowodów cyfrowych (np. na miejscu zdarzenia, w trakcie przeszukania mieszkania/firmy), mający na celu wstępne zabezpieczenie najistotniejszych, wstępnie określonych informacji (np. plików zawierających znany CSAEM w oparciu o wartości hash), zanim zostaną przeprowadzone zaawansowane, czasochłonne badania (np. przez biegłego z zakresu informatyki).

Automatyzacja pracy w hotline

Dyżurnet.pl – przez dwadzieścia lat nieprzerwanej działalności – przeszedł długą drogę: od kilkuosobowego zespołu reagującego na pierwsze w polskim internecie zgłoszenia do działającej na arenie międzynarodowej organizacji, w której wykorzystanie zaawansowanych technologii do analizy treści stanowi standard codziennej pracy ekspertów.

Podobny potencjał dostrzegany jest również w obszarze reagowania na nielegalne i szkodliwe treści w internecie. W niektórych rozwiązaniach technologicznych widoczna jest realna możliwość odciążenia analityków i usprawnienia procesów pracy, co w praktyce może przełożyć się na zwiększenie szybkości reakcji na treści nielegalne, szkodliwe oraz te wymagające bezzwłocznych działań.

Rosnąca liczba zgłoszeń oraz rozwój możliwości techniczne przyczyniły się do powstania narzędzi wspomagających pracę analityków. Coraz doskonalsze technologie hashy (odcisk cyfrowy) pozwalają ograniczyć ekspozycję analityków na materiały już znane i sklasyfikowane jako niepożądane. Metody takiej pracy są rozwijane przez zespoły analityczne Policji – zarówno krajowe, jak i międzynarodowe, oraz zespoły zrzeszone w stowarzyszeniu INHOPE.

Wykorzystanie algorytmów AI do wspomagania procesu decyzyjnego podczas klasyfikacji materiałów przedstawiających dziecko w kontekście seksualnym wciąż stanowi wyzwanie dla rozwiązań opracowywanych przez Dyżurnet.pl we współpracy z naukowcami.

Rozpoznanie i odpowiednie oznaczenie szkodliwości treści, przy szerokim katalogu materiałów – zarówno nielegalnych jak i legalnych, lecz nieprzeznaczonych dla dzieci – nie jest w pełni możliwe. Dlatego kluczowe znaczenie mają działania analityków Dyżurnet.pl, którzy obserwują trendy, nie tylko na pojedynczych platformach, lecz także identyfikują zjawiska obecne w szerszym środowisku cyfrowym, stanowiące zagrożenie dla wielu młodych użytkowników.

Rozwój sztucznej inteligencji doprowadził do powstania nowych zagrożeń

Generatywna sztuczna inteligencja otacza dziś użytkowników internetu z wielu stron – bezpośrednio, gdy korzystają z różnego rodzaju czatbotów, oraz pośrednio poprzez osoby z ich otoczenia czy liczne publikacje medialne opisujące zarówno korzyści, jak i zagrożenia wynikające z jej rozwoju. Potwierdzeniem tych zagrożeń są również zgłoszenia otrzymywane przez Dyżurnet.pl, w których widoczne jest wykorzystanie sztucznej inteligencji,

na przykład w narzędziach służących do „rozbierania" osób widocznych na zdjęciach, w tym również osób niepełnoletnich.

Duże modele językowe (ang. large language models, LLM) są szczególnie skuteczne w zadaniach, takich jak streszczanie czy klasyfikacja tekstów. Z tego powodu zdecydowano się wykorzystać zdolności AI do wychwytywania i priorytetyzacji zgłoszeń, które wymagają najszybszej reakcji. W tym celu zastosowano dostosowany **model typu Guard**, wyspecjalizowany w szybkiej klasyfikacji na podstawie wcześniej poznanych danych. **Umożliwia to wyodrębnienie spośród wielu zgłoszeń tych, które z punktu widzenia Dyżurnet.pl mają charakter priorytetowy.** Należy jednak podkreślić, że technologia ta nie jest nieomylna – dlatego **cały proces pozostaje pod nadzorem człowieka**. Ostateczne decyzje zawsze podejmowane są przez przeszkolonych specjalistów, co oznacza, że każde zgłoszenie analizowane jest przez doświadczoną osobę.

Często jednak zgłoszenie nie zawiera tekstu – przeważnie zgłaszane są treści multimedialne, takie jak obrazy czy materiały wideo. W takich przypadkach konieczne jest zastosowanie bardziej złożonego, wieloetapowego podejścia. W zasobach Zespołu Dyżurnet.pl funkcjonuje system opracowany specjalnie do celu – **APAKT** (Automatyczne Przeszukiwanie, Analiza i Klasyfikacja Treści), będący rezultatem projektu rozpoczętego w 2020 roku.

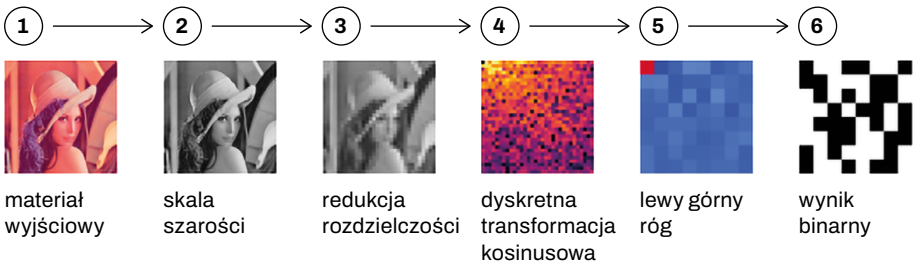
Projekt APAKT był prowadzony przez NASK – PIB przy udziale Politechniki Warszawskiej oraz firmy Enamor International Sp. z o.o. Zespół Dyżurnet.pl wraz z pracownikami naukowymi Instytutu, rozpoczął prace nad opracowaniem informatycznych narzędzi detekcji i analizy zagrożeń związanych z propagowaniem nielegalnych i wrażliwych treści w cyberprzestrzeni z wykorzystaniem modeli klasyfikacji zbudowanych przy zastosowaniu algorytmów sztucznej inteligencji. Projekt został zrealizowany w ramach programu badawczo-rozwojowego Narodowego Centrum Badań i Rozwoju – CyberSecIdent, ukierunkowanego na podniesienie bezpieczeństwa cyberprzestrzeni RP poprzez zwiększenie dostępności rozwiązań sprzętowych i programistycznych.

Po tym, gdy materiał wizualny trafi do systemu APAKT, rozpoczyna się jego automatyczna analiza. Jednym z pierwszych kroków jest obliczenie tzw. funkcji skrótu, czyli **wartości hash** – unikalnego ciągu znaków, który działa jak cyfrowy odcisk palca pliku.

System porównuje skrót z wewnętrzną bazą danych. Jeśli znajdzie identyczny hash, oznacza to, że materiał był już wcześniej analizowany i odpowiednio sklasyfikowany przez analityka. Dzięki temu nie ma potrzeby ponownego

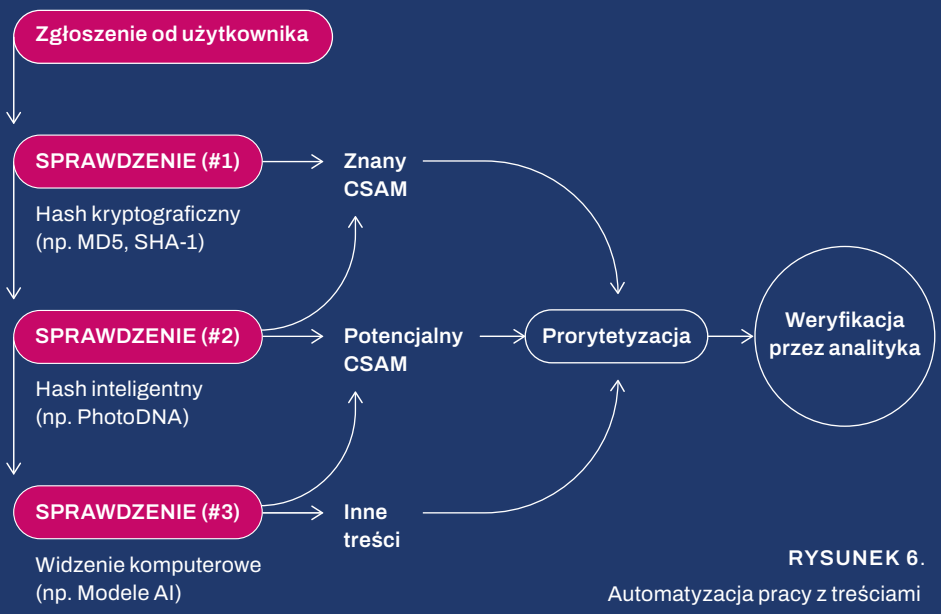
oglądania tej samej treści. Pozwala to szybko oddzielić tzw. **znane materiały CSAM** od tych, które pojawiają się po raz pierwszy i wymagają dalszej analizy.

Treści w internecie bywają jednak modyfikowane – czasem wystarczy zmiana jednego piksela, aby tradycyjny hash zmienił się całkowicie, choć obraz dla ludzkiego oka wygląda identycznie. W takich przypadkach pomocne są **percepcyjne funkcje skrótu**, które analizują ogólne cechy obrazu, takie jak kształty czy kontrasty. Dzięki temu system potrafi wykryć obrazy bardzo podobne wizualnie, nawet jeśli zostały nieznacznie zmienione.



RYSUNEK 5. Schemat przetwarzania obrazu w hash

Jeśli porównanie skrótów nie przynosi wyników, materiał trafia do kolejnego etapu analizy. Wykorzystywane są wtedy narzędzia **widzenia komputerowego (*computer vision*)**, które na podstawie wyuczonych wzorców mogą wskazać, co prawdopodobnie przedstawia obraz lub materiał wideo. Taka wskazówka pomaga analitykowi szybciej określić priorytet zgłoszenia i przygotować się na treść, którą za chwilę zobaczy.



RYSUNEK 6. Automatyzacja pracy z treściami CSAM. Źródło: opracowanie własne

Znaczna część analizowanych materiałów trafia następnie do właściwych organów ścigania jako treści nielegalne lub szkodliwe. Są to często materiały drastyczne i obciążające emocjonalnie. Dlatego każda technologia, która pozwala ograniczyć ekspozycję analityków na takie treści, a jednocześnie nie obniża jakości pracy, ma ogromną wartość.

Narzędzia takie jak modele językowe wspierające analizę zgłoszeń, funkcje skrótu czy systemy widzenia komputerowego pomagają działać szybciej i skuteczniej. **Ostateczna decyzja zawsze należy jednak do człowieka. To przeszkolony analityk ocenia kontekst i podejmuje decyzję o dalszych działaniach. Automatyzacja wspiera jego pracę, ale jej nie zastępuje.**

Projekt polskiej regulacji wspomagającej analizę CSAM przez Policję

> **Projekt ustawy dotyczącej utworzenia i funkcjonowania baz hashy stanowi ważny i długo oczekiwany krok w kierunku skuteczniejszego przeciwdziałania rozpowszechnianiu materiałów przedstawiających seksualne wykorzystywanie dzieci (CSAM) w internecie. Tego typu bazy od lat stanowią jedno z kluczowych narzędzi wykorzystywanych na świecie do szybkiego identyfikowania i blokowania znanych nielegalnych treści, a także do ograniczania ich dalszego rozpowszechniania. W Dyżurnet.pl wielokrotnie podkreślano znaczenie takich rozwiązań dla bezpieczeństwa dzieci w sieci oraz potrzebę stworzenia odpowiednich ram prawnych umożliwiających ich skuteczne wykorzystanie. Dyżurnet.pl aktywnie uczestniczy w towarzyszących projektowi pracach oraz konsultacjach, dzieląc się doświadczeniem w obszarze identyfikowania i analizowania nielegalnych treści w internecie.**

Rządowe Centrum Legislacji we wrześniu 2025 roku poinformowało o rozpoczęciu prac nad projektem Ustawy o krajowym systemie przetwarzania, analizy i klasyfikacji treści przedstawiających seksualne wykorzystywanie małoletnich:

> *Projekt ustawy zakłada wprowadzenie przepisów regulujących funkcjonowanie krajowego systemu przetwarzania, analizy i klasyfikacji treści przedstawiających seksualne wykorzystywanie małoletnich, który składać będzie się z dwóch zintegrowanych ze sobą podsystemów: podsystemu wymiany informacji o wartościach hash, czyli sygnaturach cyfrowych identyfikujących materiały przedstawiające seksualne wykorzystywanie małoletnich, zwanego dalej „bazą hash CSAM", oraz podsystemu treści przedstawiających wykorzystywanie*

seksualne dzieci, czyli bazy wizerunków osób pokrzywdzonych i sprawców, zwanej dalej „bazą zobrazowań CSAM”[15].

Celem projektu jest utworzenie dwóch zintegrowanych, odrębnie zarządzanych baz danych – **bazy hash CSAM** oraz **bazy zobrazowań CSAM** – które mają umożliwić:

- priorytetyzację działań nakierowanych na identyfikację zagrożonych dzieci (*victim-centered approach*),
- (semi)zautomatyzowaną, szybką identyfikację materiałów CSAM,
- ograniczenie kosztów i czasu wynikających z powielania czynności operacyjnych i/lub procesowych (np. wielokrotne kategoryzowanie i klasyfikowanie przez specjalistów czy biegłych treści CSAM, które znane są od kilku a nawet kilkunastu lat),
- skuteczniejsze ściganie sprawców przestępstw seksualnych wobec małoletnich.

Zjawiska **wykorzystywania seksualnego dzieci** stanowią jedną z bardziej dynamicznie rozwijających się form motywowanej finansowo (lub osobiście) zorganizowanej przestępczości internetowej (por. IOC)[16]. Stanowią one wyzwanie dla krajowych organów ścigania (Policja), wymiaru sprawiedliwości (prokuratura i sądy) oraz podmiotów odpowiedzialnych za ochronę dzieci w cyberprzestrzeni (Dyżurnet.pl). Projektowane bazy CSAM – jako zaawansowane rozwiązanie teleinformatyczne – mają stanowić odpowiedź na rosnące od lat zagrożenie przestępczością seksualną wobec dzieci.

Według informacji udostępnianych przez Policję, Dyżurnet.pl, NCMEC czy INHOPE[17], zgłoszenia dotyczące Polski obejmują m.in. przypadki:

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

16 Europol, (I)OCTA Reports (1999–2025) https://www.europol.europa.eu/publications-events/main-reports.

17 Raporty CBZC, Dyżurnet.pl, Global Child Exploitation Policy:
- https://cbzc.policja.gov.pl/bzc/statystyka/raporty-z-dzialalnosci/262,Raporty-z-dzialalnosci.html;
- https://dyzurnet.pl/publikacje;
- https://www.globalchildexploitationpolicy.org/data-insights/poland;
- https://inhope.org/articles/inhope-annual-report-2024.

- produkcji i publikowania nowych treści;
- krajowej i transgranicznej wymiany materiałów CSAM;
- deklarowania (np. na zamkniętych forach darkweb) zamiaru wykorzystania seksualnego małoletnich.

Polska znajduje się w obszarze zainteresowania siatek przestępczych zaangażowanych w handel ludźmi, monetyzację znanych materiałów CSAM oraz wytwarzanie nowych treści – w tym z korzystaniem z narzędzi AI i płatnych transmisji seksualnego wykorzystywania dzieci (*live streaming*). Potwierdzają to liczne operacje międzynarodowe prowadzone na terenie kraju[18].

Obecnie w Polsce nie funkcjonuje ogólnokrajowy system teleinformatyczny umożliwiający automatyczne sprawdzenie, czy dany materiał był wcześniej skategoryzowany jako CSAM. Wynika to m.in. z faktu, że przetwarzanie, analiza i klasyfikacja materiałów CSAM nie posiada kontratypu kodeksowego. Oznacza to, że ww. czynności są nielegalne poza: bieżącymi postępowaniami karnymi, archiwami spraw zakończonych, bazami pozakrajowymi zasilonymi przez polskie organy ścigania (np. Interpol ICSE). W praktyce prowadzi to do wielokrotnej analizy tych samych treści przez biegłych, specjalistów, prokuratorów, a nawet sędziów, co wydłuża znacząco czas postępowań karnych, utrudnia skuteczną ochronę małoletnich oraz generuje dające się wykluczyć lub zminimalizować koszty (finansowe lub osobowe).

Projektowana **baza hash CSAM**, zarządzana przez NASK – PIB i Dyżurnet.pl, będzie stosowała *hashe* kryptograficzne i perceptualne. Sygnatury *hash* umożliwią szybkie porównywanie treści zgłaszanych do Dyżurnet.pl oraz automatyczne wykrywanie materiałów już znanych.

Baza zobrazowań CSAM, zarządzana przez Komendanta Głównego Policji, będzie zawierać próbki materiałów audiowizualnych w postaci plików. Jej cel to ułatwienie identyfikacji pokrzywdzonych i sprawców, wsparcie pracy specjalistów i biegłych oraz usprawnienie czynności operacyjno-rozpoznawcze i/lub dochodzeniowo-śledcze. Dzięki centralizacji zasobów możliwe będzie bardziej efektywne zagospodarowanie kadr, środków finansowych oraz wiedzy eksperckiej. Ze względu na wrażliwość danych dostęp do bazy będzie ściśle ograniczony, a system zostanie wyposażony w zaawansowane zabezpieczenia, takie jak segmentacja, szyfrowanie, kontrolowane środowisko przetwarzania, analizy i klasyfikacji oraz pełne logowanie aktywności użytkowników.

18 Doniesienia prasowe:
- https://www.europol.europa.eu/media-press/newsroom/news/over-30-potential-victims-identified-in-action-against-human-trafficking-enabled-online;
- https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material;

Wdrożenie obu baz umożliwi integrację z systemami międzynarodowymi, takimi jak Interpol ICSE czy bazy NCMEC. Projektowana ustawa przygotowuje również Polskę do implementacji nadchodzącej unijnej legislacji dotyczącej zwalczania wykorzystywania seksualnego dzieci.

System będzie pełnił m.in. funkcje ochronne, reaktywne, wykrywcze i badawcze. Pozwoli: zapobiegać wtórnej wiktymizacji pokrzywdzonych, szybciej usuwać nielegalne treści z internetu, identyfikować zorganizowane grupy przestępcze, a także przygotowywać statystyki i analizy dotyczące obecnych i przyszłych zagrożeń.

Kampania „Dzieciństwo wolne od podtekstów", czyli jak chronić dzieci w cyfrowej rzeczywistości?

W odpowiedzi na rosnące zagrożenia związane z obecnością dzieci w internecie Dyżurnet.pl zainicjował kampanię społeczną „Dzieciństwo wolne od podtekstów", której celem było zwiększenie świadomości rodziców i opiekunów na temat bezpiecznego publikowania wizerunku dzieci w sieci. Jednym z poruszanych w niej zjawisk był sharenting – termin powstały z połączenia angielskich słów *share* (dzielić się) i *parenting* (rodzicielstwo). Oznacza on nadmierne udostępnianie w internecie zdjęć, filmów i informacji dotyczących życia dziecka, często bez jego zgody lub świadomości.

Choć publikowanie fotografii z rodzinnych uroczystości, wakacji czy codziennych chwil wydaje się naturalnym elementem korzystania z mediów społecznościowych, może wiązać się z poważnymi konsekwencjami dla prywatności i bezpieczeństwa dziecka. Raz opublikowane materiały tworzą trwały cyfrowy ślad, nad którym dziecko nie ma kontroli i który może pozostać w sieci przez wiele lat. W niektórych przypadkach takie treści mogą zostać wykorzystane w sposób niepożądany – na przykład do cyberprzemocy, manipulacji wizerunkiem czy rozpowszechniania w nieodpowiednich kontekstach.

Kampania „Dzieciństwo wolne od podtekstów" została uruchomiona w sierpniu 2025 roku – w okresie wakacyjnym, kiedy rodziny szczególnie chętnie dzielą się w internecie zdjęciami i relacjami z wyjazdów. Jej celem było zwrócenie uwagi na to, że publikowanie wizerunku dzieci w sieci wymaga większej rozwagi i refleksji nad możliwymi konsekwencjami. Kampania podkreślała, że dzieciństwo powinno kojarzyć się przede wszystkim z bezpieczeństwem i beztroską, a nie z ryzykiem kontaktu z nieodpowiednimi treściami czy niechcianą ekspozycją w sieci.

W ramach działań zorganizowano konferencję prasową oraz debatę ekspertów z udziałem przedstawicieli instytucji publicznych, organizacji pozarządowych i środowiska naukowego. Podczas spotkania omawiano zagrożenia związane z publikowaniem wizerunku dzieci w internecie, a także sposoby ich ograniczania poprzez edukację i odpowiedzialne korzystanie z mediów społecznościowych. Równolegle prowadzono działania informacyjne w internecie – przygotowano materiały edukacyjne, wywiady eksperckie, podcasty oraz treści publikowane w mediach społecznościowych. Łącznie informacje związane z kampanią dotarły do ponad 1,5 miliona użytkowników internetu.

Jednym z kluczowych przesłań kampanii było podkreślenie roli dorosłych w kształtowaniu bezpiecznego środowiska cyfrowego dla dzieci. Współczesne dzieci dorastają w rzeczywistości, w której granica między światem offline i online praktycznie nie istnieje – ich życie, relacje i aktywność przenikają się w obu tych przestrzeniach. Dlatego tak ważne jest, aby rodzice i opiekunowie byli świadomi konsekwencji publikowania treści z udziałem dzieci oraz podejmowali decyzje z uwzględnieniem ich dobra i przyszłej prywatności.

Kampania zachęcała także do reagowania na niepokojące sytuacje w sieci oraz zgłaszania treści, które mogą naruszać bezpieczeństwo lub godność dzieci. Podkreślano, że zgłoszenia przekazywane do Dyżurnet.pl pozwalają na szybsze identyfikowanie i usuwanie nielegalnych lub szkodliwych materiałów z internetu, a także na podejmowanie działań edukacyjnych mających na celu zapobieganie podobnym sytuacjom w przyszłości.

Od „notice and take down” do „order and enforce” – nowe polskie regulacje jako realne wzmocnienie DSA i ochrony dzieci w Polsce

Wdrażanie w Polsce przepisów wynikających z rozporządzenia o usługach cyfrowych (DSA) to ważny krok w kierunku skuteczniejszego reagowania na nielegalne i szkodliwe treści w internecie. Nowe regulacje wprowadzają bardziej przejrzyste procedury oraz wzmacniają współpracę między instytucjami i platformami internetowymi. Dla Dyżurnet.pl oznacza to możliwość szybszego działania i większą efektywność w reagowaniu na treści zagrażające bezpieczeństwu dzieci w sieci.

Wprowadzenie – DSA jako test skuteczności państwa

Rozporządzenie 2022/2065 – Akt o usługach cyfrowych (Digital Services Act, DSA) miało zakończyć epokę trudnej do egzekwowania odpowiedzialności platform internetowych za treści użytkowników. W centrum reformy znalazły się przejrzystość, egzekwowalność i wzmocnienie pozycji państw członkowskich wobec globalnych dostawców usług cyfrowych. Jednak DSA – jako rozporządzenie – wymaga wdrożenia krajowych ram proceduralnych, aby stać się realnym narzędziem ochrony użytkowników.

Polskie projekty nowelizacji Ustawy o świadczeniu usług drogą elektroniczną (uśude) stanowią próbę włączenia DSA w instrumenty krajowe. Szczególnym testem ich skuteczności jest to, w jaki sposób realizują poziom ochrony dzieci w internecie – obszar, w którym czas reakcji i siła egzekucji mają kluczowe znaczenie.

System nakazowy – wdrożenie art. 9 i 10 DSA

Jednym z filarów DSA są art. 9 i 10, przewidujące możliwość wydawania przez właściwe organy krajowe nakazów:

- podjęcia działań przeciwko nielegalnym treściom,
- przekazania określonych informacji o użytkownikach.

Dotychczas w polskim porządku prawnym brakowało ogólnej, horyzontalnej podstawy prawnej umożliwiającej wydawanie takich nakazów wobec dostawców usług pośrednich. Istniały rozwiązania sektorowe (np. dotyczące treści terrorystycznych czy nadużyć w komunikacji elektronicznej), lecz brakowało spójnego mechanizmu odpowiadającego konstrukcji DSA.

Projekt nowelizacji uśude wprowadza rozdział 2a ustanawiający formalną procedurę nakazową. Uprawnione podmioty – prokurator, Policja, organ Krajowej Administracji Skarbowej, uprawnieni z tytułu praw autorskich lub praw pokrewnych oraz usługobiorca – mogą wystąpić o wydanie nakazu uniemożliwienia dostępu do treści wyczerpujących znamiona określonych czynów zabronionych. W katalogu tych czynów znajdują się m.in. przestępstwa przeciwko wolności seksualnej i obyczajności, w tym czyny dotyczące seksualnego wykorzystywania małoletnich.

To jakościowa zmiana modelu regulacyjnego. System przechodzi od konstrukcji „notice and take down” – opartej głównie na zgłoszeniu i autonomicznej decyzji platformy – do modelu „order and enforce”, w którym państwo dysponuje władczym instrumentem ingerencji.

Koordynator Usług Cyfrowych i krajowa architektura egzekucyjna

Nowelizacja uśude służy również stosowaniu DSA poprzez doprecyzowanie kompetencji organów krajowych, w tym Prezesa Urzędu Komunikacji Elektronicznej w roli Koordynatora Usług Cyfrowych (Digital Services Coordinator). Ustanowienie jasnych procedur certyfikacji podmiotów pozasądowego rozstrzygania sporów, przyznawania statusu zaufanego podmiotu sygnalizującego (*trusted flagger*) oraz zweryfikowanego badacza wzmacnia instytucjonalne zaplecze egzekwowania rozporządzenia.

W praktyce oznacza to, że DSA przestaje być wyłącznie zbiorem obowiązków nakładanych na platformy, a staje się częścią **krajowego systemu nadzoru i kontroli**. Dla ochrony dzieci ma to znaczenie fundamentalne, ponieważ skuteczność regulacji zależy nie od samego brzmienia przepisów, lecz od zdolności państwa do ich wyegzekwowania.

Zaufane podmioty sygnalizujące (*trusted flagger*) i rola wyspecjalizowanych podmiotów

Art. 22 DSA ustanawia instytucję tzw. zaufanego podmiotu sygnalizującego (*trusted flagger*), przyznawaną podmiotom dysponującym szczególną wiedzą ekspercką oraz działającym w sposób obiektywny, niezależny i staranny. Zgłoszenia dokonywane przez takie podmioty muszą być przez platformy internetowe traktowane priorytetowo i rozpatrywane „bez zbędnej zwłoki". W praktyce oznacza to wzmocnienie profesjonalnych mechanizmów identyfikowania treści nielegalnych oraz zwiększenie skuteczności ich szybkiego usuwania.

Projektowane przepisy krajowe doprecyzowują tryb przyznawania, zawieszania i cofania statusu trusted flaggera, co ma istotne znaczenie dla podmiotów wyspecjalizowanych w zwalczaniu najpoważniejszych kategorii nielegalnych treści, w tym materiałów przedstawiających seksualne wykorzystywanie dzieci (CSAM). Jasne określenie procedur oraz nadzoru nad tym statusem zwiększa przejrzystość systemu i stabilność współpracy między podmiotami eksperckimi a platformami.

Z perspektywy ochrony małoletnich kluczowe jest jednak to, że DSA opiera się na zasadzie pierwszeństwa mechanizmów platformowych. Podstawową i najszybszą ścieżką eliminowania treści naruszających prawo – w szczególności treści krzywdzących dzieci – pozostaje bezpośrednia reakcja dostawcy usługi hostingowej po otrzymaniu zgłoszenia w trybie art. 16 lub art. 22 DSA. Model operacyjny powinien zatem zakładać: identyfikację nielegalnej treści przez wyspecjalizowany podmiot (np. Dyżurnet.pl), niezwłoczne przekazanie zgłoszenia platformie oraz szybkie usunięcie materiału. Taka sekwencja

działań ogranicza czas dostępności treści, minimalizuje ryzyko ich dalszego rozpowszechniania oraz redukuje skalę wtórnej wiktymizacji dziecka.

Dopiero w przypadku braku skutecznej reakcji platformy, odmowy usunięcia treści albo stwierdzenia powtarzalnych lub systemowych naruszeń obowiązków wynikających z DSA, uzasadnione jest uruchomienie ścieżki publicznoprawnej. Wówczas właściwy organ – działając na podstawie art. 9 DSA oraz przepisów krajowych – może wydać formalny nakaz podjęcia określonych działań wobec konkretnej treści. Interwencja administracyjna ma zatem charakter subsydiarny i egzekucyjny: stanowi narzędzie zapewniające skuteczność systemu w sytuacji jego niewydolności na poziomie platformy.

Tak ukształtowany model – oparty na szybkim reagowaniu platform wspieranym przez wyspecjalizowane podmioty eksperckie oraz zabezpieczony możliwością interwencji organu publicznego – najpełniej realizuje cele DSA w obszarze ochrony dzieci w internecie. Zapewnia on równowagę między odpowiedzialnością dostawców usług a rolą państwa jako gwaranta egzekwowania prawa, jednocześnie wzmacniając profesjonalne mechanizmy przeciwdziałania najpoważniejszym formom nadużyć wobec małoletnich w środowisku cyfrowym.

Ochrona małoletnich – od deklaracji do mechanizmu

DSA w art. 28 nakłada na platformy obowiązek zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich. Jednak bez krajowych narzędzi nadzoru obowiązki te mogłyby pozostać w sferze deklaratywnej.

Nowe przepisy wzmacniają ochronę dzieci w trzech wymiarach:

1. **Egzekucja wobec treści nielegalnych**
   Wprowadzenie procedury nakazowej obejmującej m.in. przestępstwa seksualne wobec małoletnich umożliwia szybszą reakcję na przypadki CSAM czy groomingu.

2. **Wzmocnienie pozycji użytkownika**
   Projekt ustawy przewiduje możliwość składania skarg na działalność usługodawców do właściwego organu oraz dochodzenia odszkodowania przed sądem powszechnym. Dzieci i ich opiekunowie uzyskują realne narzędzia prawne.

3. **Priorytetyzacja zgłoszeń**
   Obowiązek zapewnienia priorytetowego traktowania zgłoszeń od zaufanych podmiotów sygnalizujących wzmacnia skuteczność reagowania na najbardziej szkodliwe treści.

Co się realnie zmienia?

Przed wejściem w życie nowych przepisów reakcja na nielegalne treści w dużej mierze zależała od polityk moderacyjnych platform. Państwo ingerowało głównie w ramach postępowań karnych, które – z natury – są czasochłonne.

Po wdrożeniu nowych regulacji:

- organ administracyjny może wydać formalny nakaz,
- platforma ma obowiązek jego wykonania,
- brak wykonania może wiązać się z sankcją.

To przesunięcie ciężaru z samoregulacji na model współodpowiedzialności, w którym państwo posiada realny wpływ na środowisko cyfrowe.

Wyzwania

Mimo istotnego wzmocnienia systemu, kilka kwestii pozostaje otwartych i wymaga od podmiotów zajmujących się bezpieczeństwem dzieci w cyberprzestrzeni wypracowania z platformami skutecznych metod działania.

Po pierwsze, brak wyraźnej, ustawowej „pilnej ścieżki" dla spraw dotyczących dzieci oraz do działania w trybie niebezpieczeństwa bezpośredniego zagrożenia życia (ang. immediate risk to life). W praktyce skuteczność ochrony małoletnich zależy od szybkości działania – w szczególności w przypadkach transmisji na żywo czy dynamicznie rozpowszechnianych materiałów.

Po drugie, wyzwaniem pozostaje egzekucja wobec podmiotów spoza Unii Europejskiej. DSA wprowadza mechanizmy współpracy transgranicznej, jednak ich skuteczność będzie zależeć od praktyki stosowania.

Wnioski

Nowe projekty nowelizacji ustawy o świadczeniu usług drogą elektroniczną nie ograniczają się do formalnego wdrożenia DSA, lecz budują krajową architekturę jego stosowania. Wprowadzają realne instrumenty egzekucyjne, wzmacniają rolę wyspecjalizowanych podmiotów oraz przesuwają punkt ciężkości z dobrowolnej moderacji na model odpowiedzialności regulacyjnej.

Z perspektywy ochrony dzieci jest to krok w kierunku systemowego podejścia do bezpieczeństwa cyfrowego. Państwo zyskuje narzędzia do szybszego

reagowania na nielegalne treści, a eksperckie podmioty – formalne umocowanie w strukturze egzekucyjnej.

Ostateczna skuteczność nowych przepisów zależeć będzie od ich praktycznego stosowania: szybkości procedur, koordynacji między organami oraz zdolności do egzekwowania decyzji wobec globalnych platform. Rozporządzenie DSA otworzyło nowy rozdział regulacji usług cyfrowych. Nowe polskie przepisy mogą sprawić, że rozdział ten będzie miał realne znaczenie dla bezpieczeństwa najmłodszych użytkowników internetu.

Nowe trendy i zagrożenia

Boty groomingujące – nowe zagrożenie w erze sztucznej inteligencji

Sztuczna inteligencja jest dziś obecna niemal w każdej sferze życia – od inteligentnych zegarków i lodówek, przez pojazdy autonomiczne i wyszukiwarki internetowe, po gotowe modele służące do generowania obrazu, tekstu czy muzyki. Coraz częściej pojawia się również w grach online i mediach społecznościowych, gdzie funkcjonują tzw. boty konwersacyjne, określane także jako „asystenci", „towarzysze gry", „chat friend" czy „AI companion".

Badacze zwracają uwagę, że informacje przekazywane podczas rozmów między botami a dziećmi – lub osobami podszywającymi się pod dzieci – mogą stanowić zagrożenie dla szeroko rozumianego dobra małoletnich. W literaturze opisuje się m.in. zjawisko text-based child sexual abuse, czyli prowadzenia rozmów o charakterze seksualnym z dziećmi (lub na temat dzieci) przy użyciu narzędzi opartych na sztucznej inteligencji.

Jednym z przykładów opisanych w mediach były ustalenia organizacji Internet Watch Foundation (IWF), przywołane przez „The Guardian"[19]. Analitycy IWF wskazali na strony internetowe oferujące chatboty odgrywające role dzieci lub nastolatków w scenariuszach o charakterze seksualnym[20]. W niektórych przypadkach chatbot wcielał się w rolę dziewczynki, a użytkownik – osoby dorosłej. Scenariusze obejmowały m.in. historie dotyczące uwięzionej dziewczynki czy bezdomnej nastolatki zaproszonej do domu nieznajomego.

19 *Chatbot site depicting child sexual abuse images raises fears over misuse of AI*. The Guardian. https://www.theguardian.com/technology/2025/sep/21/chatbot-site-depicting-child-sexual-abuse-images-raises-fears-over-misuse-of-ai

20 *AI chatbots and child sexual abuse: A wake-up call for urgent safeguards. Internet Watch Foundation*. https://www.iwf.org.uk/news-media/blogs/ai-chatbots-and-child-sexual-abuse-a-wake-up-call-for-urgent-safeguards/

Z ustaleń IWF wynika, że dostęp do takich chatbotów był promowany w mediach społecznościowych poprzez reklamy i linki prowadzące do wybranych sekcji stron internetowych. Jednocześnie inne części tych samych serwisów oferowały legalne scenariusze rozmów o charakterze erotycznym lub neutralnym. Według analizy organizacji dostęp do witryny był możliwy z terytorium Wielkiej Brytanii, natomiast infrastruktura techniczna i podmioty odpowiedzialne za stronę znajdowały się w innych krajach. Sprawa została przekazana organizacji National Center for Missing & Exploited Children (NCMEC), która powiadomiła właściwe organy ścigania.

Kolejne przykłady dotyczą wykorzystania chatbotów w popularnych usługach internetowych. Według doniesień medialnych boty wprowadzane do komunikatorów i platform społecznościowych mogą prowadzić rozmowy z użytkownikami w sposób symulujący relacje społeczne, a w niektórych sytuacjach – także relacje romantyczne. W analizie organizacji ParentsTogetherAction[21] przeprowadzono serię kontrolowanych konwersacji, w których badacze podszywali się pod osoby małoletnie. W jednym z przypadków chatbot doradził czternastoletniej dziewczynce spotkanie z dorosłym mężczyzną poznanym w sieci, opisując szczegółowo przebieg takiego spotkania.

Raport wskazuje również na przypadki normalizowania relacji romantycznych lub seksualnych między dorosłymi a dziećmi, stosowania języka odwołującego się do emocji oraz symulowania zachowań charakterystycznych dla groomingu.

Wraz z rozwojem tego typu technologii coraz więcej uwagi poświęca się również zabezpieczeniom wbudowanym w modele językowe. Badania pokazują jednak, że mechanizmy bezpieczeństwa mogą być w niektórych sytuacjach osłabiane lub obchodzone poprzez określone sposoby prowadzenia rozmowy. W literaturze opisuje się m.in. wykorzystywanie niejednoznacznych pytań, scenariuszy symulacyjnych czy dopasowywanie tonu rozmowy w sposób prowadzący model do generowania treści naruszających zasady bezpieczeństwa[22].

Przykłady te pokazują, że rozwój generatywnej sztucznej inteligencji stwarza nowe wyzwania dla systemów ochrony dzieci w internecie. Technologie konwersacyjne mogą być wykorzystywane nie tylko do celów edukacyjnych czy rozrywkowych, lecz także do tworzenia treści lub scenariuszy, które mogą stanowić zagrożenie dla najmłodszych użytkowników sieci.

21 *Meta AI chatbots present grooming and sexual exploitation risks*. https://parentstogetheraction.org/2025/04/28/meta-ai-chatbots-present-grooming-and-sexual-exploitation-risks/

22 APGardaí. (2025). *Under the hood: Can AI chatbots facilitate* [Substack newsletter]. Substack. https://apgardai.substack.com/p/under-the-hood-can-ai-chatbots-facilitate

Gdy sieć rani – o cyberprzemocy wśród dzieci i młodzieży

Cyberprzemoc rówieśnicza pozostaje jednym z najczęstszych zagrożeń, z jakimi dzieci i młodzież spotykają się w internecie. Wraz z rozwojem mediów społecznościowych i komunikatorów zmieniają się jednak jej formy – coraz częściej przybierają one postać nowych trendów i wyzwań krążących w sieci. Dla młodych użytkowników mogą one wyglądać jak element internetowej zabawy, w rzeczywistości jednak często prowadzą do ośmieszania, wykluczania i publicznego poniżania rówieśników. Przykładem takiego zjawiska jest trend określany jako „szon patrole", który w 2025 roku zwrócił uwagę analityków Dyżurnet.pl.

„Szon patrole" – to trend w mediach społecznościowych, który zyskał popularność wśród dzieci i młodzieży w Polsce w 2025 roku. W przestrzeni publicznej pojawiły się doniesienia opowiadające o nim, jako o nowym zjawisku, jednak analiza Działu Dyżurnet.pl potwierdziła, że to kolejny przykład cyberprzemocy rówieśniczej. Niekiedy określanej jako *cyberbullying* lub nękanie w sieci.

Definicja i formy cyberprzemocy

Cyberprzemoc to przemoc z użyciem urządzeń elektronicznych[23] – np. telefonów komórkowych, laptopów, tabletów – oraz internetu. Analogicznie jak w przypadku tzw. tradycyjnych form przemocy charakteryzuje ją: nierównowaga sił między sprawcą a osobą pokrzywdzoną oraz regularnie podejmowane działań jednej z osób, których celem jest skrzywdzenie drugiej osoby. Zjawisko to przybiera różne formy. Wśród nich wyróżnić można:

- **agresję słowną** – np. publikowanie obraźliwych i wulgarnych komentarzy lub postów, wyzywanie w wiadomościach przesyłanych za pomocą komunikatorów, groźby karalne;
- **publikowanie kompromitujących materiałów** – zdjęć lub nagrań, które mają charakter poniżający dla osoby na nich przedstawionej, są publikowane bez jej zgody, niekiedy mogą zostać zmodyfikowane np. za pomocą narzędzi z wbudowaną sztuczną inteligencją;
- **cyberprzemoc o charakterze seksualnym** – w tym szantaż na tle seksualnym i publikowanie intymnych materiałów danej osoby bez jej zgody;

23 Strona internetowa Cyberprofilaktyka: https://cyberprofilaktyka.pl/blog/cyberprzemoc---czym-jest-i-jak-rozmawiac-o-niej-z-dzieckiem_i27.html

- **kradzież tożsamości** – bezprawne pozyskanie oraz posługiwanie się danymi osobowych lub innymi informacjami (w tym np. profilami czy kontami w mediach społecznościowych lub grach online) pozwalającymi na podszywanie się pod daną osobę;

- **wykluczanie z grupy rówieśniczej** – np. poprzez tworzenie na komunikatorze grupy zamkniętej, do której wstęp jest ograniczony tylko dla jednej osoby w klasie;

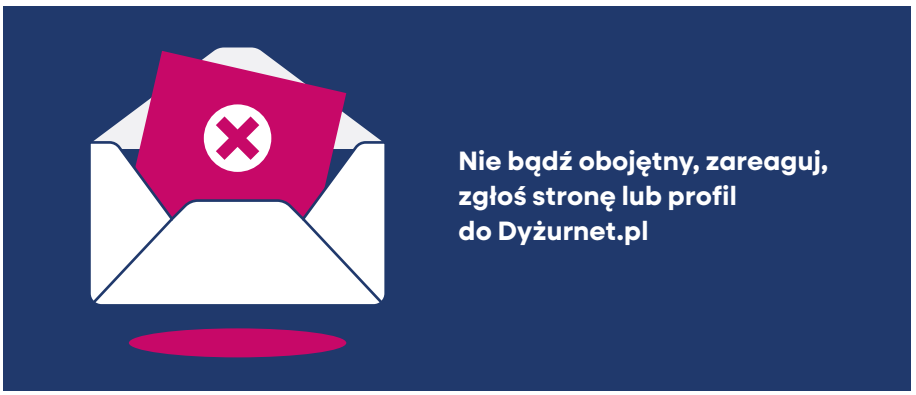
- **tworzenie tzw. *hate pages*** – zakładanie profili w mediach społecznościowych, których celem jest wyłącznie publikowanie treści poniżających wybraną osobę.

W sprawach związanych z cyberprzemocą dochodzi również do upublicznienia danych osobowych osoby doświadczającej hejtu, a czasem i jej najbliższych. W sieci pojawiają się informacje, w tym dotyczące miejsca ich zamieszkania, co w kontekście kierowania gróźb karalnych związanych z użyciem przemocy wywołuje realne poczucie zagrożenia.

Na jednym z portali, który umożliwia tworzenie quizów online m.in. związanych z różnymi dziedzinami nauki, opublikowano poniżające, ośmieszające zagadki na temat jednego dziecka. Obok wulgarnych odpowiedzi dodano kompromitujące zdjęcia przedstawiające jego wizerunek. Po działaniach podjętych przez Dział Dyżurnet.pl materiał został usunięty ze strony.

Skala zjawiska cyberprzemocy wobec dzieci i nastolatków

Dyżurnet.pl otrzymuje liczne zgłoszenia dotyczące różnych form cyberprzemocy od osób jej doświadczających, a także ich rodziców, opiekunów lub szkolnych pedagogów.



Z najnowszego badania *Nastolatki* realizowanego przez NASK w 2024 roku wynika, że 29% dzieci i młodzieży doświadczyło w świecie wirtualnym wyzywania, 19% ośmieszania, 18% poniżania, 13% szantażowania. Badacze zwracają również uwagę na 17% deklaracji „trudno powiedzieć", co może wynikać z problemu jednoznacznego zidentyfikowania i nazwania, z jakim zjawiskiem badany miał do czynienia[24]. To niepokojące dane, które mogą świadczyć o niskiej świadomości problemu cyberprzemocy oraz o coraz większych trudnościach dzieci i młodzieży w rozpoznawaniu jej form.

Z badania wynika również, że dla co dziesiątego nastolatka doświadczenie cyberprzemocy miało charakter cykliczny, a nie incydentalny. 10% dzieci i młodzieży wskazywało, że doświadcza tego raz lub kilka razy w miesiącu, a 7% raz lub kilka razy w tygodniu[25].

Szon patrole

Dyżurnet.pl w 2025 roku otrzymał wiele zgłoszeń dotyczących profili w mediach społecznościowych określonych, jako „szon patrol". Po analizie treści dostępnych na zgłoszonych kontach oraz bieżącym monitoringu, zjawisko to zaklasyfikowano jako formę cyberprzemocy rówieśniczej, czyli cyberprzemoc stosowaną przez dziecko lub nastolatka wobec jego rówieśnika. Celem ataków był wygląd fizyczny – to także najczęstszy deklarowany powód cyberprzemocy w badaniu *Nastolatki*[26].

Nastolatki zakładały anonimowe konta, aby obrażać i poniżać rówieśników. Charakterystyczną cechą tych profili były nazwy, w których łączono krzywdzące i wulgarne określenie – „szony" (słowo używane wobec dziewcząt), „babiarze" i „cwele" (wobec chłopców) – z nazwą miejscowości lub szkoły. Publikowano na nich zdjęcia poszczególnych dzieci, bez ich zgody, a także obraźliwe opisy i komentarze. Organizowano nawet konkursy na „największego szona" lub „babiarza".

Konta najczęściej były prywatne, w związku z czym dostęp do nich był ograniczony. W ten sposób dzieci i młodzież skutecznie ukrywały przemocowe treści przed rodzicami, opiekunami oraz nauczycielami. Dyżurnet.pl regularnie zgłaszał konta dotyczącego tego trendu bezpośrednio do administratora serwisu w celu ich zablokowania.

24 Ładna, A., (red.). (2025). N*astolatki. Raport z ogólnopolskiego badania uczniów i rodziców*. NASK – Państwowy Instytut Badawczy, s. 68–69.

25 Tamże, s. 73.

26 Tamże, s. 75.

Reakcja dzieci i nastolatków na przemoc

Niepokojącym jest fakt, że aż 47% badanych dzieci i nastolatków, które doświadczyło cyberprzemocy, nie poinformowało o tym nikogo[27]. W konsekwencji mierzyli się oni z tą trudną sytuacją w samotności i bez wsparcia bliskich lub osób świadczących pomoc psychologiczną.

19% szukało pomocy wśród znajomych, a zaledwie 15% wśród rodziców lub opiekunów prawnych[28]. Jeszcze mniej osób postanowiło zgłosić sprawę administratorowi serwisu lub portalu, psychologowi, pedagogowi szkolnemu, bądź nauczycielowi.

To alarmujące dane, które mogą wskazywać na brak zaufania do osób dorosłych i instytucji.

Skutki cyberprzemocy

Doświadczenie cyberprzemocy powoduje szereg negatywnych konsekwencji. Dziecko może odczuwać smutek i lęk, mieć zaniżone poczucie własnej wartości i problemy z samooceną. Niekiedy będzie ograniczało kontakty z innymi osobami (np. rówieśnikami, rodziną) i stopniowo izolowało się od poszczególnych grup. Mogą pojawić się również konsekwencje somatyczne m.in. ból brzucha, problemy ze snem. Długotrwałe narażenie na cyberprzemoc może skutkować depresją, myślami rezygnacyjnymi i zachowaniami suicydalnymi.

Jak rozmawiać z dziećmi i nastolatkami, które doświadczyły cyberprzemocy?

- Powstrzymaj się od negatywnej oceny i nie obwiniaj dziecka za sytuację, w której się znalazło. To dla niego trudny moment, w którym potrzebuje wsparcia i zrozumienia. Gdy poczuje się odrzucone przez najbliższą mu osobę (np. rodzica, opiekuna), może stracić zaufanie i samotnie mierzyć się z problemami, jakich doświadcza – niekiedy reagując w sposób autodestrukcyjny.

- Wspólnie zastanówcie się, jakie działania należy podjąć. Porozmawiaj z dzieckiem o możliwości zgłoszenia cyberprzemocy do administratora serwisu lub portalu, do Dyżurnet.pl, a także do organów ścigania (Policja) i wymiaru sprawiedliwości (prokuratura).

27 Tamże, s. 76.

28 Tamże, s. 77.

- Powiadom dziecko o możliwości profesjonalnego wsparcia psychologicznego, na przykład o Telefonie zaufania dla dzieci i młodzieży 116 111, prowadzonym przez Fundację Dajemy Dzieciom Siłę. Linia jest całodobowa, bezpłatna i anonimowa. Cenne może okazać się również wsparcie długoterminowe w postaci terapii.

Pamiętaj! Jeśli zauważyłeś w sieci cyberprzemoc – np. obraźliwe, poniżające, wulgarne komentarze – reaguj i zgłoś to do administratora serwisu lub do Dyżurnet.pl (Uwaga! nie jest istotne, czy serwis jest polski, czy zagraniczny). Taki sprzeciw wobec hejtu w internecie to jasny sygnał, który może przyczynić się do usunięcia treści z portalu.

Szkodliwe treści na wygasłych domenach placówek edukacyjnych

> **W 2025 roku Dyżurnet.pl otrzymał zgłoszenia dotyczące szkodliwych treści publikowanych pod adresami internetowymi, które wcześniej należały do placówek edukacyjnych. Analiza wykazała, że problem wynikał z przejmowania wygasłych domen szkolnych przez inne podmioty. W efekcie użytkownicy – w tym uczniowie i ich rodzice – mogli trafiać na strony zawierające nieodpowiednie treści.**

Analiza wykazała, że wskazane adresy internetowe w przeszłości należały do szkół, które zaprzestały prowadzenia swoich stron internetowych i nie przedłużyły abonamentu na posiadane domeny. Placówki te zdecydowały się na uruchomienie nowych witryn pod innymi adresami, pozostawiając dotychczasowe domeny bez odnowienia. W rezultacie domeny te mogły zostać ponownie zarejestrowane przez inne podmioty.

Zgłoszone adresy najczęściej zawierały nazwę placówki lub jej skrót oraz nazwę miejscowości, w której szkoła funkcjonowała. Domeny zawierające elementy geograficzne są często wyszukiwane przez użytkowników internetu, dzięki czemu generują znaczną liczbę odsłon. Z tego powodu są one atrakcyjne dla firm lub osób zajmujących się wykupywaniem wygasłych domen. W niektórych przypadkach takie adresy są następnie wykorzystywane do publikowania treści szkodliwych.

Użytkownicy odwiedzający dawny adres strony szkoły byli automatycznie przekierowywani na strony pornograficzne. Problem potęgował fakt, że wyszukiwarki internetowe nadal kierowały użytkowników do poprzednich adresów stron, które ze względu na swoją charakterystyczną budowę i utrwaloną obecność w sieci pozostawały wysoko pozycjonowane w wynikach wyszukiwania.

Istotnym elementem mechanizmu było to, że w części przypadków przekierowanie następowało jedynie w przypadku wejścia na stronę z poziomu wyszukiwarki internetowej. Przy bezpośrednim wpisaniu adresu w przeglądarce wyświetlana była jedynie standardowa informacja o domenie wystawionej na sprzedaż. Tego rodzaju działanie utrudnia wykrycie problemu oraz jego szybką identyfikację przez administratorów.

Sytuacja ta narażała odwiedzających strony – wśród których znaczną część mogą stanowić uczniowie oraz ich rodzice – na niezamierzoną ekspozycję na treści pornograficzne. W odpowiedzi na zgłoszenia Zespół Dyżurnet.pl podjął działania polegające na zablokowaniu dostępu do wskazanych treści w ramach Ogólnopolskiej Sieci Edukacyjnej

Opisane przypadki pokazują, jak istotne jest odpowiedzialne zarządzanie domenami internetowymi przez podmioty prowadzące działalność edukacyjną. Nawet po zakończeniu korzystania z danej domeny warto rozważyć jej dalsze utrzymywanie lub odpowiednie przekierowanie, aby ograniczyć ryzyko wykorzystania jej w sposób mogący narazić użytkowników – w tym dzieci i młodzież – na kontakt ze szkodliwymi treściami.

Współpraca z Partnerami

> **Dyżurnet.pl prowadzi nie tylko działania związane z reagowaniem na nielegalne treści w internecie, ale również aktywnie angażuje się w działalność edukacyjną. Jednym z elementów tej misji jest upowszechnianie wiedzy na temat bezpiecznego korzystania z sieci poprzez publikacje, kampanie społeczne oraz programy informacyjne dotyczące zagrożeń online i sposobów ich ograniczania. Organizowane są także szkolenia, konferencje, seminaria oraz zajęcia edukacyjne skierowane do różnych grup odbiorców, m.in. uczniów, nauczycieli, funkcjonariuszy organów ścigania oraz przedstawicieli wymiaru sprawiedliwości.**

Trzy dni intensywnego szkolenia o zwalczaniu seksualnego wykorzystywania dzieci w cyberprzestrzeni

W dniach 5–7 listopada 2025 roku w Lublinie odbyło się trzydniowe szkolenie poświęcone zwalczaniu seksualnego wykorzystywania dzieci w cyberprzestrzeni. Szkolenie zostało przeprowadzone przez ekspertów Dyżurnet.pl oraz Centralnego Biura Zwalczania Cyberprzestępczości Policji, na zaproszenie Krajowej Szkoły Sądownictwa i Prokuratury i było skierowane do prokuratorów, sędziów oraz kuratorów.

Program obejmował szerokie spektrum zagadnień – od form seksualnego wykorzystywania dzieci w dobie nowych technologii, takich jak grooming, szantaż na tle seksualnym czy transmisje na żywo, po problematykę treści CSAM, w tym materiałów generowanych i przetwarzanych z użyciem sztucznej inteligencji. Istotnym elementem szkolenia była również odpowiedzialność platform internetowych, regulacje prawne oraz granice tej odpowiedzialności w kontekście ochrony prywatności i szyfrowania komunikacji.

Uczestnicy zapoznali się z metodami działania sprawców w internecie, procedurami analitycznymi, współpracą międzynarodową oraz narzędziami informatyki śledczej używanymi podczas przeszukań i zabezpieczania dowodów cyfrowych. Duży nacisk położono na praktyczne aspekty identyfikacji ofiar groomingu i szantażu na tle seksualnym, klasyfikację materiałów CSAM oraz przygotowanie i ocenę materiału dowodowego, w tym z użyciem narzędzi automatyzacji i AI.

Szczególną wartością szkolenia była możliwość bezpośredniej wymiany wiedzy i doświadczeń pomiędzy różnymi uczestnikami postępowania przygotowawczego i karnego – przedstawicielami Policji, prokuratury, sądów oraz ekspertami. Ten dialog pozwolił nie tylko na lepsze zrozumienie wzajemnych ról i ograniczeń, lecz także zaowocował konkretnymi pomysłami na nowe działania i inicjatywy, które mogą przyczynić się do skuteczniejszego wykrywania, ścigania i zapobiegania przestępstwom seksualnym wobec dzieci w przyszłości.

Ważną częścią szkolenia była również perspektywa osób pokrzywdzonych – omówiono skutki wykorzystywania seksualnego dzieci oraz konsekwencje upubliczniania treści, podkreślając znaczenie podejścia skoncentrowanego na pokrzywdzonym w postępowaniu karnym. Całość stanowiła przykład kompleksowego i interdyscyplinarnego podejścia do jednego z najpoważniejszych wyzwań współczesnego wymiaru sprawiedliwości – ochrony dzieci przed przemocą seksualną w środowisku cyfrowym.

Seksualne wykorzystywania dzieci w cyberprzestrzeni z perspektywy kodeksu rodzinnego i opiekuńczego

W 2025 roku eksperci Dyżurnet.pl wzięli udział w dwóch przedsięwzięciach organizowanych przez środowisko sędziów zajmujących się kompleksowo sprawami dotyczącymi rodziny (procedujących w oparciu o ustawę z dnia 25 lutego 1964 roku Kodeks rodzinny i opiekuńczy, Dz. U. 1964 Nr 9 poz. 59, z późn. zm.). Inicjatywa ta będzie kontynuowana w 2026 roku w ramach kolejnych wspólnych wydarzeń, takich jak webinary, szkolenia, konferencje. Dyżurnet.pl dzięki wymianie wiedzy i współpracy z sędziami rodzinnymi, poszerza dotychczasowe obszary reagowania na zjawisko krzywdzenia dzieci o cenną perspektywę osób mających bezpośredni wgląd w sytuację rodzinną

i dobrostan dzieci. W dłuższej perspektywie, ta pozyskana wiedza ekspercka pozwoli sprawniej systemowo reagować, zanim dziecko stanie się pokrzywdzonym w rozumieniu przepisów Kodeksu karnego. Nowe kierunki współpracy, wymiany wiedzy i doświadczeń obejmują trzy obszary:

- ochronę małoletnich pokrzywdzonych w wyniku czynów zabronionych (w tym przez rówieśników);
- nieletnich sprawców czynów zabronionych związanych z przemocą seksualną w sieci;
- metodykę pracy sędziego w sprawie dotyczących małoletnich i nieletnich (obszar obejmuje: technologie, współpracę z Dyżurnet.pl, dostawcami usług oraz organami ścigania, jak również dobre praktyki i procedury).

Celem rozwijanych kierunków współpracy jest zachęcenie do współpracy prokuratorów, sędziów, policjantów oraz pozostałych ekspertów zajmujących się szeroko rozumianą ochroną dzieci w cyberprzestrzeni oraz do wymiany doświadczeń zarówno z Dyżurnet.pl, jak również między sobą.

Wydarzenia

16–17.01	warsztaty dla uczniów szkół podstawowych i liceów w Poznaniu dotyczących zagrożeń związanych z publikacją wizerunku w internecie
5.02	udział w spotkaniu w ramach projektu CYBERspoty – „Ciemna strona internetu: jak radzić sobie z nielegalnymi i szkodliwymi treściami online i gdzie je zgłaszać?”
19.03, 9.04	wystąpienie „Ryzykowne zachowania online” podczas konferencji „Szanse, wyzwania, zagrożenia – wprowadzenie do problematyki bezpieczeństwa dzieci i młodzieży online”
20.03	warsztaty CyberBaza – treści nielegalne i szkodliwe w internecie, Wrocław
10.04	warsztaty CyberBaza – grooming i zachowania ryzykowne w sieci
16.04	warsztaty w ramach projektu CYBERspoty – „Grooming i utrata kontroli nad zdjęciami: Jak chronić siebie i innych?”
16–17.09	warsztaty „Ryzykowne zachowania i kontakty online, publikacja materiałów intymnych, treści nielegalne i szkodliwe” w ramach szkolenia z zaawansowanych kompetencji cyfrowych dla służb mundurowych w Warszawie
26.09	webinar „Patotreści 2.0” w ramach 19. Międzynarodowej Konferencji „Bezpieczeństwo dzieci i młodzieży w internecie” 2025
21–22.10	warsztaty „Ryzykowne zachowania i kontakty online, publikacja materiałów intymnych, treści nielegalne i szkodliwe” w ramach szkolenia z zaawansowanych kompetencji cyfrowych dla służb mundurowych w Tychach

6–7.11 warsztaty „Ryzykowne zachowania i kontakty online, publikacja materiałów intymnych, treści nielegalne i szkodliwe” w ramach szkolenia z zaawansowanych kompetencji cyfrowych dla służb mundurowych w Poznaniu

18–19.11 warsztaty „Ryzykowne zachowania i kontakty online, publikacja materiałów intymnych, treści nielegalne i szkodliwe” w ramach szkolenia z zaawansowanych kompetencji cyfrowych dla służb mundurowych w Gdańsku

25.11 warsztaty „Treści szkodliwe w internecie – jak reagować i zapobiegać” w ramach szkolenia dla Komendy Wojewódzkiej Policji w Bydgoszczy

2–3.12 warsztaty „Ryzykowne zachowania i kontakty online, publikacja materiałów intymnych, treści nielegalne i szkodliwe” w ramach szkolenia z zaawansowanych kompetencji cyfrowych dla służb mundurowych w Warszawie

3.12 warsztaty „Treści nielegalne i szkodliwe w internecie” w ramach szkolenia dla Komendy Wojewódzkiej Policji w Krakowie

15.12 warsztaty „Treści szkodliwe, w tym patotreści” w ramach szkolenia dla Komendy Miejskiej Policji w Olsztynie

16.12 prowadzenie warsztatów „Treści szkodliwe, w tym patotreści” w ramach szkolenia dla Komendy Wojewódzkiej Policji w Olsztynie

Wydarzenia organizowane przez NASK – PIB we współpracy z Fundacją Wspierania i Rozwoju Młodzieży ADYS

13.05 warsztaty dla Fundacji ADYS – grooming i zachowania ryzykowne w sieci

20.05 warsztaty dla Fundacji ADYS – treści nielegalne i szkodliwe w internecie

Wydarzenia organizowane przez podmioty zewnętrzne

5.03 wystąpienie „Prywatność oraz zachowania ryzykowne w sieci" podczas konferencji „Dzień Bezpiecznego Internetu. Łódzkie 2025" – organizator: Urząd Marszałkowski Województwa Łódzkiego

9.04 webinar Rodzic 3.0 – jak chronić dziecko przed zagrożeniami w internecie (cyberprzemoc, pornografia), organizator: Warszawskie Centrum Innowacji Edukacyjno-Społecznych i Szkoleń (WCIES)

15.05 wystąpienie na temat groomingu podczas konferencji „Bezpieczne dzieci w sieci", organizator: Urząd Miasta w Ostrowcu Świętokrzyskim

23.05 „Mowa nienawiści obecna w cyberprzestrzeni", konferencja – wdrożenie nowej kampanii Wydziału Prewencji Komendy Wojewódzkiej Policji w Katowicach „Jesteśmy różni, ale równi", organizator: Wydział Prewencji Komendy Wojewódzkiej Policji w Katowicach

29.10 wykład „Bezpieczeństwo w sieci i cyberzagrożenia. Szkoła bez hejtu: budowanie kultury szacunku i dialogu" w ramach konferencji Regionalne Forum Edukacji, organizator: Województwo Małopolskie i Kuratorium Oświaty w Krakowie

19.11 prelekcja na temat roli hotline'ów w reagowaniu na CSAM i udział w panelu dyskusyjnym konferencji „System ochrony dzieci przed przemocą seksualną w Polsce", organizator: Państwowa Komisja do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15

4.12 webinar Rodzic 3.0 – jak chronić dziecko przed zagrożeniami w internecie (cyberprzemoc, pornografia), organizator: Warszawskie Centrum Innowacji Edukacyjno-Społecznych i Szkoleń (WCIES)

10.12 wykład „Cyberprzemoc a wykorzystywanie seksualne dzieci i młodzieży" w ramach konferencji „Poznać i zrozumieć. STOP wykorzystywaniu seksualnemu dzieci i młodzieży", organizator: Komenda Powiatowa Policji w Starych Babicach

O NASK

NASK jest Państwowym Instytutem Badawczym nadzorowanym przez Ministra Cyfryzacji.

Cyberbezpieczeństwo i ochrona użytkowników oraz działania związane z zapewnieniem bezpieczeństwa są kluczowym polem aktywności NASK. Reagowaniem na zdarzenia naruszające bezpieczeństwo sieci i przyjmowaniem zgłoszeń o naruszeniach zajmuje się Zespół CERT Polska (www.cert.pl) oraz Dyżurnet.pl. Zgodnie z Ustawą o krajowym systemie cyberbezpieczeństwa NASK – PIB został wskazany na poziomie krajowym jako jeden z trzech Zespołów Reagowania na Incydenty Komputerowe, tzw. CSIRT, który koordynuje obsługę incydentów zgłaszanych przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać wszyscy użytkownicy internetu.

NASK współtworzy również zaplecze analityczne oraz badawczo-rozwojowe dla Krajowego Systemu Cyberbezpieczeństwa, prowadzi działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Działalność naukowo-badawcza NASK ma również wymiar wdrożeniowy i prorynkowy. W Instytucie badacze ujmują komercyjny problem w ramy nauki, by za pomocą jej narzędzi, nierzadko szerszych i bardziej abstrakcyjnych, dojść do wyników nie tylko satysfakcjonujących, ale również innowacyjnych. Główny nurt badań wyznacza cyberbezpieczeństwo, rozumiane jako wykrywanie, ostrzeganie, reagowanie na incydenty, pozyskiwanie, analiza, przetwarzanie i transfer danych, a także złożone systemy sieciowe, w tym systemy IoT oraz mobilne sieci ad hoc. Obecnie w badaniach rozwijany jest obszar sztucznej inteligencji. Istotne miejsce zajmują badania dotyczące biometrycznych metod weryfikacji tożsamości w bezpieczeństwie usług. Jako operator telekomunikacyjny NASK oferuje innowacyjne rozwiązania teleinformatyczne dla klientów finansowych, biznesowych, administracji i nauki. NASK prowadzi także rejestr nazw w domenie *.pl* (www.dns.pl).

Słownik pojęć

APAKT
projekt, którego celem jest Automatyczne Przeszukiwanie, Analiza i Klasyfikacja Treści. Stworzone narzędzie identyfikuje materiały przedstawiające seksualne wykorzystywanie dzieci – zarówno te już rozpoznane i sklasyfikowane w przeszłości, jak i zupełnie nowe.

baseline
kryterium opisujące materiały CSAM, które stanowią treść nielegalną we wszystkich krajach zrzeszonych w INHOPE.

baza hashy
podsystem wymiany informacji o wartościach *hash*, czyli cyfrowych sygnaturach identyfikujących materiały przedstawiające seksualne wykorzystywanie małoletnich, wykorzystywany do ich wykrywania i usuwania bez konieczności przetwarzania samych obrazów.

baza wizerunków
podsystem zawierający treści przedstawiające seksualne wykorzystywanie dzieci, obejmujący zobrazowania osób pokrzywdzonych i sprawców, służący analizie, klasyfikacji oraz wsparciu identyfikacji ofiar i sprawców przestępstw seksualnych wobec małoletnich.

CSAM
child sexual abuse material – materiały przedstawiające seksualne wykorzystywanie dziecka. Kategoryzowane przez ekspertów Dyżurnet.pl jako treści pornograficzne z udziałem małoletnich (art. 202 k.k.).

CSEM
child sexual exploitation material – materiały prezentujące dziecko w seksualnym kontekście, będące nadużyciem wobec dziecka, jednak w większości krajów, w tym w Polsce, uznawane za legalne.

incydent
zgłoszenie poddane analizie oraz odpowiednio zaklasyfikowane przez ekspertów Dyżurnet.pl.

INHOPE
sieć zaufanych zespołów reagujących, której celem jest eliminacja materiałów przedstawiających seksualne wykorzystywanie dzieci oraz wsparcie krajowych procedur na rzecz jak najszybszego usuwania nielegalnych materiałów. Działalność towarzyszenia jest wspierana przez Interpol, Europol, Virtual Task Force, European Financial Coalition, INSAFE,

generatywna sztuczna inteligencja
generative artificial intelligence – technologia umożliwiająca tworzenie nowych treści lub modyfikowanie istniejących na podstawie danych zgromadzonych wcześniej do jej wytrenowania.

hash
sygnatura pliku, jego „cyfrowy odcisk palca".

ICCAM
baza wymiany informacji dotyczących CSAM dostępna dla zespołów zrzeszonych w INHOPE, do której na bieżąco przekazywane są materiały zaklasyfikowane jako przedstawiające seksualne wykorzystanie dziecka.

ICSE
International Child Sexual Exploitation database – utrzymywana przez Interpol baza, do której przekazywane są informacje o najbardziej drastycznych materiałach w kategorii CSAM, dzięki czemu możliwe jest podjęcie działań w celu identyfikacji zarówno ofiar, jak i sprawców.

trusted flagger
podmiot posiadający status zaufanego podmiotu sygnalizującego na podstawie DSA, którego zgłoszenia dotyczące nielegalnych treści są traktowane priorytetowo przez platformy internetowe ze względu na wykazaną wiedzę i kompetencje.

Universal Classification Schema
uniwersalny schemat klasyfikacji treści stanowiący wspólny zestaw kategorii i kryteriów umożliwiających jednolite oznaczanie, analizę i wymianę informacji o materiałach CSAM pomiędzy różnymi systemami i instytucjami.

victim-centered approach
podejście skoncentrowane na osobie pokrzywdzonej, zakładające priorytetowe uwzględnianie bezpieczeństwa, praw, godności i dobrostanu ofiary na każdym etapie działań instytucji i organów prowadzących sprawę.

zgłoszenie
powiadomienie dotyczące potencjalnie nielegalnych treści w internecie przesłane przez użytkownika lub instytucję.

NASK

WYDAWCA

NASK – Państwowy Instytut Badawczy

ul. Kolska 12
01-045 Warszawa

e-mail: info@nask.pl
info@dyzurnet.pl

ISSN 2084-7785