CZARNA KSIĘGA MŁODYCH OFIAR PLATFORM CYFROWYCH W POLSCE



Ministerstwo
Cyfryzacji

CZARNA KSIĘGA MŁODYCH OFIAR PLATFORM CYFROWYCH W POLSCE

Krzywda dzieci i odpowiedzialność platform

listopad 2026

Ministerstwo Cyfryzacji

ZAMIAST WSTĘPU

Szanowny Panie Prezydencie,

Zwracam się dziś do Pana nie tylko jako do głowy państwa, w której rękach spoczywa decyzja o przyszłości prawa, które może chronić miliony Polek i Polaków. Zwracam się do Pana także jako do ojca, bo gdy rozmawiamy o bezpieczeństwie dzieci w internecie, za nazwami ustaw, przepisami i politycznymi sporami kryje się doświadczenie, które każdy rodzic potrafi sobie wyobrazić.

Dziecko, które nie chce rano wyjść do szkoły, bo ktoś rozesłał jego intymne zdjęcie kolegom i koleżankom. Ktoś inny grozi, że pokaże następne. Telefon, który miał ułatwić kontakt z przyjaciółmi, nagle staje się źródłem strachu. Rodzice próbują zatrzymać przemoc, ale nie wiedzą, do kogo się zwrócić. A platforma, na której wszystko się wydarzyło, odsyła ich do kolejnego formularza.

Panie Prezydencie, to nie jest odosobniony obraz. Przygotowana przez nas „Czarna księga młodych ofiar platform cyfrowych w Polsce" pokazuje, jak wielka jest skala tego problemu i jak często pozostaje on niewidoczny, nawet dla najbliższych.

W badaniu NASK 39% nastolatków zadeklarowało doświadczenie co najmniej jednej z badanych form przemocy internetowej. Wśród 1439 uczniów, którzy potwierdzili takie doświadczenie, aż 47% przyznało, że nic z tym nie zrobiło i nikomu o nim nie powiedziało[1]. W innym badaniu, dotyczącym cyberagresji seksualnej, 70,7% pokrzywdzonych nie ujawniło nikomu najbardziej dotkliwego incydentu[2].

Za tymi liczbami stoi młody człowiek, który może codziennie spotykać prześladowcę w szkole, a po powrocie do domu – nadal otrzymywać jego wiadomości. Przemoc cyfrowa nie kończy się wraz z ostatnią lekcją – dociera także do dziecięcego pokoju, który powinien dawać poczucie bezpieczeństwa. Proszę pomyśleć, co oznacza dla dziecka brak miejsca, w którym może od tej przemocy odpocząć.

Przez lata powtarzaliśmy rodzicom, że powinni rozmawiać z dziećmi, kontrolować ich aktywność i uczyć je odpowiedzialności. To nadal waż-

ne. Ale dziś wiemy, że odpowiedzialność rodziny i szkoły nie wystarczy. Nie można oczekiwać, że rodzice samodzielnie ochronią dzieci przed zagrożeniami wynikającymi z funkcjonowania globalnych platform technologicznych, których zasady działania pozostają często poza ich wiedzą i kontrolą.

To właśnie dlatego Europa zdecydowała się zmienić reguły gry.

Akt o usługach cyfrowych, znany jako DSA, wyraża zasadę: wielkie platformy cyfrowe muszą ponosić odpowiedzialność za bezpieczeństwo usług, które projektują i udostępniają milionom ludzi. Nie wystarczy reagować, gdy wydarzy się tragedia. Trzeba rozpoznawać zagrożenia, ograniczać ryzyko i projektować usługi tak, aby bezpieczeństwo użytkowników, szczególnie dzieci, było nieodłączną cechą tych usług.

Panie Prezydencie, proszę zauważyć, jak głęboka jest to zmiana. Przez lata przyzwyczajano nas do przekonania, że internet jest przestrzenią, w której odpowiedzialność spoczywa przede wszystkim na użytkowniku. Tymczasem to platformy decydują, jakie treści zobaczymy, kto będzie mógł się z nami kontaktować, co zostanie nam polecone i jak łatwo będzie rozpowszechnić materiał naruszający czyjąś godność.

To nie są neutralne decyzje technologiczne – mają realne konsekwencje dla ludzkiego życia.

W naszej publikacji pokazujemy również, że zagrożenia dotyczą dzieci coraz młodszych. Według raportu „Internet dzieci" około 760 tys. dzieci w wieku 7–12 lat aktywnie korzystało z TikToka, a 290 tys. – z Instagrama[3]. Mówimy więc o dzieciach, których bezpieczeństwo zależy od mechanizmów zaprojektowanych przez globalne firmy.

Dziś do tych zagrożeń dochodzi sztuczna inteligencja. Zwyczajne zdjęcie może zostać wykorzystane do stworzenia fałszywego materiału intymnego. Dziecko nie musi już niczego wysyłać sprawcy, żeby stać się ofiarą szantażu czy publicznego poniżenia. Technologia rozwija się szybciej niż nasza zdolność reagowania na krzywdę, którą może wyrządzić.

Nie możemy pozwolić, żeby odpowiedzią państwa na tę rzeczywistość była bezradność. Dlatego tak ważne jest, aby Polska potrafiła w pełni wykorzystywać instrumenty przewidziane w DSA. Europejskie prawo już obowiązuje, ale jego skuteczność wymaga również sprawnych krajowych instytucji, odpowiednich procedur i rzeczywistego egzekwowania obo-

wiązków platform. Potrzebujemy rozwiązań, które pozwolą szybko reagować na nielegalne treści, skutecznie chronić najmłodszych i rozliczać dostawców usług z ich odpowiedzialności.

Wiem, że wokół tych rozwiązań toczą się polityczne spory. Wiem, że pojawiają się pytania o wolność słowa, prywatność i granice ingerencji państwa. To ważne pytania, których nie wolno lekceważyć. Ale jestem przekonany, że potrafimy chronić te wartości, nie godząc się jednocześnie na bezkarność sprawców przemocy i zaniedbania platform.

Bezpieczeństwo dzieci i wolność nie są wartościami, które musimy sobie przeciwstawiać. Przeciwnie, dziecko, które boi się przemocy, szantażu czy upokorzenia, nie jest naprawdę wolne.

Panie Prezydencie, nie zwracam się do Pana z prośbą o polityczne poparcie dla rządu. Zwracam się do Pana, bo jestem przekonany, że istnieją sprawy, w których państwo musi przemówić jednym głosem. Ochrona dzieci przed przemocą cyfrową jest jedną z nich.

Nie oczekuję, że jeden podpis rozwiąże wszystkie problemy. Ale wiem, że bez odważnych decyzji i skutecznego prawa nie zbudujemy systemu, który będzie chronił dzieci przed zagrożeniami współczesnego świata.

Proszę więc Pana, abyśmy wspólnie wzięli za to odpowiedzialność.

Na końcu tej historii nie ma europejskiego rozporządzenia, politycznego sporu ani kompetencji kolejnej instytucji. Jest dziecko, które czeka na pomoc. Jest rodzic, który chce je ochronić. I jest państwo, które musi udowodnić, że potrafi stanąć po ich stronie.

Panie Prezydencie, dzieci nie mogą czekać, aż dorośli zakończą swoje polityczne spory.

Na koniec chcę podziękować wszystkim organizacjom społecznym, instytucjom, badaczkom i badaczom, którzy od lat monitorują zagrożenia w świecie cyfrowym, prowadzą badania, przygotowują raporty i konsekwentnie budują debatę publiczną o bezpieczeństwie dzieci i odpowiedzialności platform cyfrowych. Szczególnie dziękuję tym, których badania i analizy wykorzystaliśmy w tej publikacji. Bez Waszej pracy wiele dramatów dzieci pozostałoby niewidocznych, a wiele zagrożeń nigdy nie zostałoby właściwie rozpoznanych i nazwanych. Wasze raporty, badania i codzienna działalność nie tylko dostarczają nam

wiedzy i podnoszą świadomość społeczną. Są także źródłem inspiracji i motywują mnie do jeszcze cięższej pracy, odważniejszych decyzji i większej determinacji w egzekwowaniu odpowiedzialności od największych platform cyfrowych.

Jestem głęboko przekonany, że z patologiami świata cyfrowego poradzimy sobie tylko razem. Parlament, rząd, prezydent, ludzie nauki i społeczeństwo obywatelskie muszą działać wspólnie. Możemy różnić się poglądami, kompetencjami i sposobami działania, ale musi nas łączyć jeden cel: bezpieczeństwo w świecie cyfrowym. To nasza wspólna odpowiedzialność!

Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji

PLATFORMY ZWIĘKSZAJĄ SKALĘ KRZYWDY

Przemoc zyskuje na platformach zasięg

Krzywdzący materiał może powstać podczas szkolnego konfliktu, napaści, ośmieszającej sytuacji; może też zostać wykonany bez wiedzy dziecka. Może to być zdjęcie, nagranie lub obraźliwy wpis przedstawiający młodą osobę albo odnoszący się bezpośrednio do niej. Gdy materiał trafi na platformę, do poniżania dziecka dołączają kolejni użytkownicy. Pojawiają się następne komentarze, kopie i przeróbki. Dziecko mierzy się wtedy z obiegiem treści, którego nie jest w stanie kontrolować. Obieg ten odbywa się w infrastrukturze zaprojektowanej i zarządzanej przez konkretnego dostawcę usługi.

W szkolnym konflikcie znaczenie ma publiczność. Platforma może znacznie powiększyć grono odbiorców i sprawić, że nagranie, na którym uwieczniono daną sytuację, będzie rozpowszechniane długo po samym zdarzeniu. Chwila upokorzenia przestaje być epizodem, o którym wie kilka osób. Materiał może docierać do znajomych, ich kontaktów i osób całkowicie obcych. Każda z nich otrzymuje możliwość reakcji albo dalszego rozpowszechnienia pozyskanych danych. Platforma decyduje, jak łatwe są te czynności i jakie zabezpieczenia je ograniczają.

Autor obraźliwego wpisu i dostawca platformy odpowiadają za różne działania. Dostawca nie musi być autorem wpisu, aby jego zaniedbania miały znaczenie dla powstawania dalszej krzywdy. Jeśli platforma nie chroni skutecznie konta dziecka, nie reaguje na kolejne sygnały o nękaniu lub nierzetelnie rozpatruje wiarygodne zgłoszenia, trzeba sprawdzić, czy jej dostawca wypełnia swoje obowiązki. W razie potwierdzenia naruszeń platforma powinna naprawić zaniedbania i ponieść przewidziane prawem konsekwencje.

Problem zaczyna się w konstrukcji usługi

Publiczne profile, łatwość kopiowania treści, rekomendacje i kontakt z nieznajomymi mogą ułatwiać nadużycia wobec dzieci. Funkcje te mają

również użyteczne zastosowania, ale każdą z nich trzeba ocenić pod kątem bezpieczeństwa dziecka. Dostawca platformy powinien sprawdzać, czy sposób udostępniania treści i nawiązywania kontaktów w jego usłudze nie ułatwia nękania lub szantażu. Powinien także zapewniać bezpieczne ustawienia domyślne, ułatwiać blokowanie niechcianych kontaktów i sprawnie rozpatrywać zgłoszenia. Musi przy tym chronić prywatność użytkowników i poufność ich rozmów.

Poradnik NASK „Pułapki sieci. Sieć pułapek" opisuje zagrożenia związane z kontaktami z innymi użytkownikami, dostępnymi treściami, presją stałej obecności w sieci i utratą prywatności. Dziecko nie korzysta osobno z algorytmu, osobno z komunikatora i osobno z systemu zgłoszeń. Przechodzi między nimi w jednej aplikacji. Bezpieczeństwo musi być równie spójne[4].

Nieskuteczne zabezpieczenie w jednym miejscu może podważyć ochronę w pozostałych. Zablokowanie konta sprawcy nie zapewnia skutecznej ochrony, jeśli może on łatwo założyć nowe konto i ponownie kontaktować się z dzieckiem. Oznaczenie materiału jako nieodpowiedniego może ograniczyć wyświetlanie podobnych treści, ale nie gwarantuje skutecznej ochrony przed kolejnymi podobnymi rekomendacjami. Dostawca powinien wykazać, że jego zabezpieczenia współdziałają i są skuteczne także wtedy, gdy ktoś celowo próbuje je obejść. Musi też sprawdzić, czy użytkownik rozumie, jakie skutki ma wybranie opcji „Nie interesuje mnie to", a jakie zgłoszenie materiału do moderacji z powodu naruszenia zasad serwisu.

Po zgłoszeniu kończy się wymówka niewiedzy

Zgłoszenie zmienia sytuację platformy – otrzymuje ona konkretny sygnał o naruszeniu. Powinna go rozpoznać, ocenić kontekst i zastosować właściwe środki. Pokrzywdzony ma prawo oczekiwać zrozumiałego uzasadnienia decyzji oraz realnej drogi jej zakwestionowania. Automatyczna odpowiedź nie wystarczy, jeśli nękanie nadal trwa.

Kontekst jest szczególnie ważny w sytuacji przemocy rówieśniczej. Neutralne zdjęcie może zostać umieszczone na profilu służącym upokarzaniu. Pozornie zwykły komentarz może odsyłać do wcześniejszej groźby. Wiele wpisów, z których każdy osobno wygląda niepozornie, może tworzyć skoordynowany atak. Platforma, która ocenia wyłącznie pojedynczy obrazek, może przeoczyć sens całej akcji. Obowiązek poprawy takiego

systemu spoczywa na platformie.

Ośrodek Analizy Dezinformacji NASK opisał konta na Instagramie związane z tzw. szon patrolami, służące piętnowaniu dziewcząt poprzez publikowanie list ich profili. Analitycy zgłaszali te konta, wskazując kontekst nękania. Instagram część z nich usunął, ale inne zgłoszenia odrzucił mimo podobnego charakteru materiałów. Sam fakt zgłoszenia nie gwarantował ochrony. Trzeba wyjaśnić, czy moderatorzy rozumieli polskie określenia użyte w publikacjach i łączyli zgłoszenia dotyczące tej samej akcji[5].

Zgłaszając kolejną kopię krzywdzącego materiału, dziecko nie powinno opowiadać całej historii od początku. Platforma musi uwzględnić wcześniejsze zgłoszenia i kontekst sprawy oraz ograniczać dalszy obieg rozpoznanych kopii treści naruszających prawo lub regulamin. Granice tych działań wyznaczają przepisy i prawo użytkowników do prywatności. Jeśli materiał wraca, trzeba sprawdzić skuteczność zabezpieczeń.

Same statystyki nie ochronią dzieci przed krzywdą

Liczba zatrudnionych moderatorów, rozmiar regulaminu i liczba rozpatrzonych formularzy nie mówią jeszcze, czy dziecko jest bezpieczne. Potrzebne są odpowiedzi na prostsze pytania. Jak długo krzywdząca treść pozostawała dostępna po zgłoszeniu? Czy zniknęły jej rozpoznane kopie? Czy sprawca odzyskał możliwość kontaktu z pokrzywdzonym dzieckiem? Czy zmieniono błędną decyzję o odrzuceniu zgłoszenia, zanim nękanie się nasiliło? Tak wygląda rozliczanie ochrony z perspektywy pokrzywdzonego.

Akt o usługach cyfrowych DSA zobowiązuje największych dostawców usług cyfrowych do oceny i ograniczania ryzyka systemowego, w tym zagrożeń dla praw dziecka, zdrowia i dobrostanu. To podstawa badania sposobu działania całej platformy, a nie tylko pojedynczych postów. Organ nadzoru powinien sprawdzać projekt funkcji, praktykę moderacji i skuteczność środków naprawczych. Ryzyko rozpoznane na papierze musi prowadzić do zmiany w działającej usłudze[6].

Odpowiedzialność platformy zaczyna się więc przed pierwszą skargą i trwa po pierwszym usunięciu zgłoszonej treści. Obejmuje zapobieganie przewidywalnemu zagrożeniu, właściwą reakcję oraz ograniczanie powrotu naruszenia.

53 FAKTY O OFIARACH PLATFORM CYFROWYCH

01 760 tysięcy dzieci w wieku 7–12 lat na TikToku

Samo podanie wieku przy rejestracji nie wystarczy. Dostawcy powinni skutecznie egzekwować minimalny wiek zakładania kont przyjęty dla danej usługi. Oznacza to wiarygodne i proporcjonalne sprawdzanie wieku oraz blokowanie lub usuwanie kont użytkowników, którzy nie spełniają tego warunku. Sama deklaracja wieku przy rejestracji nie zapewnia skutecznego przestrzegania ograniczeń. Ochrona oparta na założeniu, że najmłodszych użytkowników po prostu nie ma, pozostawia ich bez odpowiednich zabezpieczeń.

Według raportu „Internet dzieci" z 2025 r. około 760 tys. dzieci w wieku 7–12 lat aktywnie korzystało z aplikacji TikTok na smartfonach. W tej grupie wiekowej z Instagrama korzystało około 290 tys., z Messengera około 900 tys., a z WhatsAppa około 700 tys. najmłodszych użytkowników[7].

Skala korzystania z tych aplikacji przez dzieci wymaga sprawdzenia, czy ograniczenia wieku działają w praktyce. Odpowiedzialności za ich przestrzeganie nie można przerzucać wyłącznie na dzieci i rodziców. Dostawca powinien pokazać, jak zapobiega zakładaniu i utrzymywaniu kont przez osoby poniżej wymaganego wieku.

02 To nie „internet", lecz konkretne platformy

Wśród uczestników badania Fundacji Dajemy Dzieciom Siłę „Rówieśnicy. Raport 2026 o przemocy rówieśniczej" 92% korzystało w ostatnim roku z YouTube, 77% z Messengera, 74% z TikToka, 66% z Instagrama, 65% z Robloxa, a 47% z Discorda. Zasięg obejmuje więc serwisy wideo, komunikatory, media społecznościowe i gry. W każdym z tych miejsc potrzebne są narzędzia dostosowane do wieku użytkownika i rodzaju możliwego nadużycia[8].

W grupie uczestników w wieku 10–12 lat z TikToka korzystało 54%, a z Instagrama i Facebooka po 35%. Jeśli z deklaracji dzieci wynika, że korzystają z tych aplikacji, choć są za młode, by zakładać w nich konta, platformy muszą uwzględniać tę grupę w ocenie ryzyka i skutecznie egzekwować przyjęte ograniczenia wieku[9].

Odpowiedzialności nie można rozmywać przez ogólne hasło „internet". Konkretna firma kontroluje konkretny produkt, jego ustawienia i obsługę zgłoszeń. Rodzina powinna wiedzieć, gdzie zgłosić przemoc w filmie, gdzie nękanie w komunikatorze, a gdzie naruszenie podczas gry. Każdy dostawca ma zapewnić działającą drogę interwencji i odpowiadać za jej skuteczność.

Wielu użytkowników pozostanie przy ustawieniach domyślnych z chwili zakładania konta. Przy dużym zasięgu usługi właśnie te ustawienia decydują więc o ochronie znacznej części dzieci. Odnajdywanie wszystkich opcji w kilku aplikacjach wymaga czasu i wiedzy, które nie każda rodzina ma pod dostatkiem; podstawowe zabezpieczenia nie mogą zależeć od wykonania tej pracy przez opiekunów.

03 Pierwszy kontakt z ekranem już w wieku 2 lat

Badanie „Brzdąc w sieci", przeprowadzone w 2020 r. wśród rodziców dzieci w wieku 0–6 lat, pokazało, że z urządzeń mobilnych korzystało 54% dzieci objętych badaniem. Średni wiek rozpoczęcia korzystania wynosił 2 lata i 2 miesiące. Wśród korzystających dominowały urządzenia z dostępem do internetu. To pokazuje, jak wcześnie usługi cyfrowe wchodzą do codzienności rodzin[10].

Małe dziecko nie rozpoznaje modelu reklamowego, manipulacji ani ryzyka udostępnienia danych. Nie ocenia wiarygodności obcej osoby tak jak dorosły. Jeżeli produkt trafia do jego otoczenia, zabezpieczenia powinny uwzględniać ten etap rozwoju. Określenia „dla rodziny" i „dla dzieci" powinny oznaczać także bezpieczne kontakty, treści odpowiednie do wieku, łatwe zakończenie korzystania z aplikacji oraz ograniczenie zbierania danych do niezbędnego minimum.

W ogólnopolskim badaniu NASK opisanym w raporcie „Nastolatki" 41% uczniów otrzymało pierwszy smartfon w wieku 9–10 lat, a około 40% przed dziewiątymi urodzinami. Osobisty telefon daje stały przenośny do-

stęp do aplikacji. Przestaje być urządzeniem, z którego dziecko korzysta zawsze w obecności dorosłego. Bezpieczeństwo produktu staje się w tej sytuacji jeszcze ważniejsze[11].

Własny smartfon oznacza również przeniesienie relacji rówieśniczych „do kieszeni". Grupa klasowa działa po lekcjach. Wiadomości przychodzą w drodze do domu, wieczorem i w weekend. Rodzic nie widzi wszystkich interakcji, a dziecko nie relacjonuje każdej rozmowy. Dlatego bezpieczeństwo dziecka nie może zależeć od ciągłego nadzoru opiekuna. Ochrona musi działać w samej usłudze. Dostawcy komunikatorów oferujących publiczne kanały i kontakt z nieznajomymi powinni uwzględniać ryzyko korzystania z nich przez zbyt młode osoby oraz skutecznie egzekwować przyjęte ograniczenia wieku.

04 3 godziny i 23 minuty dziennie w mediach społecznościowych

W badaniu NASK nastolatki deklarowały, że spędzają w internecie średnio 4 godziny i 59 minut dziennie w dni powszednie oraz 5 godzin i 16 minut w weekendy. Same media społecznościowe zajmowały według deklaracji nastolatków średnio 3 godziny i 23 minuty dziennie. Młody człowiek spędza zatem w tych usługach czas porównywalny z dużą częścią szkolnego dnia[12].

Gdy nastolatki poświęcają mediom społecznościowym tyle czasu, powiadomienia, rekomendacje i zasady kontaktu wpływają na rytm ich całego dnia. Platforma może utrudniać robienie przerw w korzystaniu z aplikacji albo je ułatwiać. Może domyślnie ograniczać nocne sygnały albo podtrzymywać gotowość do sprawdzania telefonu. To konkretne ustawienia – każde z nich można poddać kontroli i każdemu przypisać odpowiedzialnego dostawcę.

Raport „Internet dzieci", wykorzystujący także pomiar aktywności użytkowników, wskazuje, że w grupie wiekowej 7–14 lat dzienna aktywność w internecie wynosiła około 4 godzin i 29 minut[13].

Ten sam raport opisuje także wieczorne korzystanie z aplikacji. W dni powszednie między 21.00 a 22.00 z aplikacji internetowych choć raz korzystało około 40% dzieci w wieku 7–12 lat i blisko 70% młodzieży w wieku 13–18 lat. Wiele dzieci korzysta więc z sieci także tuż przed snem[14]. Ocena ryzyk systemowych powinna obejmować to, czy powiado-

mienia, automatyczne odtwarzanie i nieskończone przewijanie sprzyjają nadmiernemu lub kompulsywnemu korzystaniu z usług, także w porze przeznaczonej na sen.

05 Nastolatki mają średnio 6,5 konta w sieci. Rodzice są przekonani, że o połowę mniej

NASK pokazuje wyraźną różnicę między deklaracjami nastolatków dotyczącymi korzystania z mediów społecznościowych a wyobrażeniami rodziców na ten temat. Rodzice szacowali czas dziecka w mediach społecznościowych na średnio 2 godziny i 6 minut, podczas gdy uczniowie podawali 3 godziny i 23 minuty. Podobna rozbieżność dotyczyła liczby używanych kont: średnio 6,50 według nastolatków i 3,42 według rodziców[15].

Takiej luki nie zamknie sam apel o większą czujność. Rodzic może znać jedną aplikację, gdy dziecko korzysta z kilku; może widzieć profil publiczny, a nie wiedzieć o koncie służącym do kontaktów z inną grupą. Powinien łatwo ustawić zabezpieczenia i sprawdzić, które konta oraz funkcje aplikacji one obejmują.

Rozmowy i reguły również bywają postrzegane odmiennie. O ustalaniu zasad korzystania z internetu mówiło 57% rodziców i 21% nastolatków. Rozmowy o zagrożeniach deklarowała połowa rodziców, lecz dostrzegało je 15% uczniów. Włączenie filtrów i blokad wskazywało 28% rodziców i 13% nastolatków. Te wyniki pokazują, jak łatwo dorosły może przecenić zakres istniejącej ochrony[16]. Dlatego też dostawcy powinni zapewniać bezpieczne ustawienia domyślne, ograniczać ryzykowne funkcje, oferować zrozumiałe i łatwo dostępne narzędzia wspierające rodziców i nastolatków w zarządzaniu bezpieczeństwem konta.

06 13 lat w regulaminie, młodsze dzieci na platformach

Rozwiązania zapewniające odpowiedni wiek dostępu muszą być skuteczne i proporcjonalne. Dziecko nie powinno płacić za ochronę nadmiernym ujawnianiem danych o swojej tożsamości, historii korzystania z usług internetowych ani dokumentów. Europejska Rada Ochrony Danych wskazuje w tej sprawie zasady minimalizacji danych, ograniczenia celu i konieczności stosowanych środków. Dostawca powinien wykazać,

dlaczego określone dane są potrzebne i jak zapobiega ich dalszemu wykorzystaniu[17].

Sprawdzanie wieku pomaga chronić dzieci przed treściami i usługami, które nie są dla nich przeznaczone. Komisja Europejska udostępniła rozwiązanie techniczne, dzięki któremu użytkownik potwierdza osiągnięcie wymaganego wieku, nie ujawniając platformie swojej tożsamości ani daty urodzenia. W zaleceniu z 29 kwietnia 2026 r. wskazała, że takie narzędzia powinny być dostępne w państwach członkowskich do 31 grudnia 2026 r. Platformy muszą korzystać z metod, które pozwalają skutecznie egzekwować ograniczenia dostępu i jednocześnie chronią prywatność użytkowników.

Granice wieku wymagają także jasnego języka. Regulaminowe 13 lat w wielu usługach nie stanowi ogólnego prawa dziecka do każdej funkcji ani uniwersalnego progu wynikającego z RODO. Ochrona danych, dostęp do konkretnej usługi i bezpieczeństwo jej funkcji to obowiązki, które muszą działać równolegle. Rodzina powinna otrzymać zrozumiałą informację, jakie ograniczenie obowiązuje i co dostawca robi, by go przestrzegać[18].

07 39% badanych nastolatków doświadczyło przemocy w internecie. Blisko co trzeci był wyzywany

Dzięki platformom sprawca może nękać dziecko także po jego wyjściu ze szkoły. Komentarze, wiadomości i kopie nagrań docierają do telefonu w domu. Granica szkolnego dnia przestaje zatrzymywać upokorzenie. Dziecko może obawiać się każdego kolejnego powiadomienia i nie wiedzieć, kto jeszcze zobaczył kompromitujący je materiał. Aplikacja pozostaje otwarta także wtedy, gdy lekcja, przerwa i spotkanie ze sprawcą dawno się skończyły.

W badaniu NASK 39% nastolatków potwierdziło doświadczenie co najmniej jednej z badanych form przemocy internetowej. Wyzywania doświadczyło 29%, ośmieszania – 19%, poniżania – 18%, a straszenia i szantażowania po 13% badanych. To codzienny język krzywdy, która dociera do młodych użytkowników przez narzędzia komunikowania i publikowania[19].

Nie każde naruszenie staje się publiczną aferą. Część rozgrywa się w niewielkiej grupie, której wszyscy członkowie spotkają pokrzywdzonego następnego dnia. W takim otoczeniu liczba wyświetleń może być mała, ale siła upokorzenia ogromna.

08 Co miesiąc lub częściej. Przemoc w sieci wracała do niemal co czwartej ofiary

W badaniu „Nastolatki" wśród 1439 uczniów, którzy doświadczyli przemocy internetowej, 7% wskazało, że spotykało ich to raz lub kilka razy dziennie, 7% – raz lub kilka razy w tygodniu, a 10% – raz lub kilka razy w miesiącu. Łącznie daje to około 24% pokrzywdzonych doświadczających przemocy co najmniej raz w miesiącu[20].

Przy powtarzającym się nękaniu dziecko musi liczyć się z następną wiadomością lub publikacją. Po otrzymaniu zgłoszenia platforma powinna więc natychmiast ocenić wskazane treści i konta, a w razie stwierdzenia naruszenia – zastosować odpowiednie środki, np. usunąć materiał lub nałożyć ograniczenia na konto wykorzystywane do nękania.

09 Przemoc rówieśnicza przenosi się do sieci. Trzech na czterech uczestników badania doświadczyło cyberprzemocy w ciągu roku

Raport FDDS „Rówieśnicy 2026", obejmujący 141 911 uczniów w wieku 10–17 lat, pokazuje przenikanie przemocy bezpośredniej i internetowej. 58% uczestników wskazało wyśmiewanie wyglądu, 56% – nieprzyjemne wiadomości w internecie, a 53% – wykluczenie z grupy lub aktywności online. W tych doświadczeniach ciało, reputacja i przynależność do grupy stają się przedmiotem ataku[21].

Trzy czwarte uczestników tego badania doświadczyło w ostatnim roku co najmniej jednej z czterech analizowanych form cyberprzemocy. 20% wskazało doświadczenie cyberbullyingu, czyli powtarzalnej przemocy uwzględniającej przewagę sprawcy nad pokrzywdzonym. 13% przyznało się do jego stosowania. Tych wyników nie wolno sprowadzić do kilku ostrych żartów wymienionych między równymi sobie osobami. Opisują one utrwalone relacje krzywdzenia[22].

Wykluczenie z grupy internetowej może odcinać dziecko od zwykłych kontaktów z klasą. Obraźliwy wpis może poprzedzać docinki na korytarzu. Przemoc w szkole może dostarczać materiału do kolejnego nagrania. Gdy platforma traktuje każdą publikację jako osobny incydent, nie widzi ciągłości tego samego ataku.

Wyniki międzynarodowego badania HBSC opublikowane przez WHO w 2024 r. pokazują, że 15% badanych jedenasto-, trzynasto- i piętnastolatków z 44 krajów i regionów doświadczyło cyberbullyingu. Między 2018 a 2022 r. odsetek wzrósł z 12% do 15% u chłopców i z 13% do 16% u dziewcząt. To zagrożenie przekraczające granice jednej szkoły i jednego państwa. Odpowiedź na nie musi obejmować również platformy działające ponad tymi granicami[23].

10 Krótkie nagranie napaści, miesiące opresji

Komunikat Policji z Gdańska z 21 kwietnia 2026 r. opisuje przemoc wobec piętnastoletniego chłopca. Dwóch piętnastolatków i osiemnastolatka mieli się nad nim znęcać, a zdarzenie zostało zarejestrowane. Sygnał do Policji dotarł od osoby, która otrzymała pliki, i jej ojca. Nagranie pomogło uruchomić interwencję. Jego dalszy obieg mógłby jednocześnie odnawiać upokorzenie pokrzywdzonego[24].

Ten podwójny charakter materiału wymaga sprawnej procedury. Dowód powinien trafić do uprawnionych organów, a publikacja naruszająca prawa dziecka powinna zostać wycofana z publicznego obiegu w internecie. Rodzic nie może być zmuszony do wyboru między zabezpieczeniem materiału dowodowego a zatrzymaniem rozpowszechniania nagrania krzywdzącego jego dziecko.

Napaść może trwać kilka minut. Jej internetowa publiczność może wracać do niej miesiącami. Dlatego samo ukaranie sprawcy nie wystarcza do ochrony pokrzywdzonego dziecka. Dziecko potrzebuje także zatrzymania obiegu nagrania, ochrony przed komentarzami i ograniczenia możliwości ponownego publikowania rozpoznanego materiału.

11 70% badanych nastolatków widziało prawdziwą przemoc w mediach społecznościowych

Brytyjski Youth Endowment Fund w badaniu „Children, Violence and Vulnerability 2024" ustalił, że 70% badanych nastolatków z Anglii i Walii widziało w ostatnim roku w mediach społecznościowych treści przedstawiające rzeczywistą przemoc. Wśród osób z takim doświadczeniem 25% wskazywało promowanie materiału przez funkcje platform, a 6% – jego aktywne wyszukiwanie. Do kontaktu z treściami przedstawiającymi rzeczywistą przemoc dochodzi więc także podczas zwykłego korzystania z aplikacji[25].

Platforma musi brać pod uwagę użytkownika, któremu brutalna treść zostaje podsunięta. Odpowiedzialność nie kończy się na możliwości wpisania właściwego hasła w wyszukiwarkę. Dotyczy również poleceń, automatycznego odtwarzania i materiałów udostępnianych przez innych, zwłaszcza że większość dzieci trafia na takie treści przemocowe przypadkiem. Dziecko powinno móc skutecznie zatrzymać dalszą ekspozycję bez wielokrotnego oglądania podobnych scen po to, by je zgłosić.

Amerykańskie badanie podłużne Michele Ybarry, Kimberly Mitchell i Jaya Oppenheima wykazało związek między deklarowaną ekspozycją na przemoc w mediach w dzieciństwie a poważnymi zachowaniami przemocowymi 5 i 10 lat później, także po uwzględnieniu innych badanych czynników. Autorzy wskazują, że ograniczanie kontaktu dzieci z treściami przedstawiającymi przemoc może być jednym z elementów zapobiegania poważnym zachowaniom przemocowym w późniejszym życiu[26]. Dla nadzoru oznacza to konieczność badania dostępu dzieci do takich treści i sposobu ich rozpowszechniania.

Przegląd Bhavyi Shah i Pratimy Kaushik z 2025 r. zwraca z kolei uwagę na naśladownictwo, fascynację sprawcami i dostęp do wzorców działania w kulturze cyfrowej. Są to ostrzeżenia przed środowiskiem, w którym przemoc może zyskiwać uznanie i przyciągać kolejnych naśladowców[27].

12 Dwóch 16-latków w grupach ekstremistycznych. ABW ujawnia niebezpieczne kontakty na Telegramie i Discordzie

We wrześniu 2026 r. ABW poinformowała o zatrzymaniu dwóch szesnastolatków aktywnych w grupach na Telegramie i Discordzie związanych ze środowiskami neonazistowskimi i ekstremistycznymi. Analiza urządzeń zabezpieczonych w tej sprawie ujawniła m.in. materiały propagandowe oraz dotyczące zamachów i masowych zabójstw. Agencja odtwarzała kontakty i sprawdzała udział innych osób w procesie radykalizacji[28].

Kolejny komunikat w tej sprawie opisał zatrzymanie osoby, której przedstawiono m.in. zarzut przygotowywania zamachu terrorystycznego. Według ABW uczestnicy rozmów w grupach na tych samych platformach analizowali wcześniejsze zamachy, ich sprawców i możliwe ataki, traktując sprawców jako źródło inspiracji. To udokumentowany przykład wykorzystania komunikacji internetowej do budowania środowiska skupionego wokół przemocy[29].

Odrębny przypadek dotyczył publikacji groźby przemocy w szkole. W październiku 2026 r. Radio Poznań opisało interwencję w Krobi po pojawieniu się takiego nagrania. Według przytoczonej wypowiedzi rzeczniczki Policji piętnastolatek tłumaczył publikację chęcią zdobycia polubień na TikToku. Szkoła i służby musiały zareagować na realne zagrożenie[30].

13 47% nastolatków, którzy doświadczyli przemocy w internecie, nikomu o tym nie powiedziało i nie podjęło żadnych działań

W badaniu NASK 47% uczniów, którzy doświadczyli przemocy internetowej, nic z tym nie zrobiło i nikomu o niej nie powiedziało. Dziecko może obawiać się utraty telefonu, eskalacji ataku albo reakcji rówieśników. Może też nie wierzyć, że dorosły lub administracja serwisu potraktują sprawę poważnie. Takiego milczenia nie wolno przedstawiać jako dowodu, że problem nie wymaga interwencji[31].

W badaniu FDDS „Rówieśnicy 2026" wśród uczniów, którzy wiedzieli o przemocy, lecz jej nie zgłosili, 44% nie uważało sytuacji za poważną, 25% wskazało, że nie przyszło im to do głowy, 20% obawiało się zgłosze-

nia, a 11% – nie wiedziało, komu przekazać informacje[32].

Jeżeli aplikacja pokazuje formularz zgłoszenia dopiero po przejściu przez wiele menu, część młodych osób go nie odnajdzie. Jeżeli kategorie są nazwane wyłącznie językiem regulaminu użytkownik może nie dopasować do nich swojej sytuacji. Dostawca powinien uprościć odnajdywanie formularza i wybór właściwej kategorii zgłoszenia.

Szkoła ma chronić ucznia, ale nie zastąpi administracji aplikacji i platform. Nauczyciel nie usunie konta sprawcy i nie zatrzyma systemu rekomendowania nagrania. Rodzice również nie otrzymują takiej możliwości. Działania szkoły wspierające pokrzywdzonego ucznia muszą być prowadzone równolegle z działaniami platformy, które zatrzymują nękanie i rozpowszechnianie krzywdzących materiałów w jej usłudze. Bez tego współdziałania otoczenie dziecka próbuje gasić kryzys, do którego platforma nadal dostarcza paliwo.

14 45,5% badanych nastolatków doświadczyło co najmniej jednej formy cyberagresji seksualnej

Groźba publikacji zdjęcia daje sprawcy władzę nad codziennym życiem dziecka. Może on żądać następnych materiałów, pieniędzy albo wykonywania poleceń. Telefon, który służył kontaktowi z bliskimi, staje się źródłem strachu. Platforma udostępniająca narzędzia takiej komunikacji musi umieć przerwać zależność, kiedy otrzymuje sygnał o zagrożeniu.

W badaniu NASK „Agresja i przemoc seksualna w internecie” 45,5% uczniów w wieku 14–18 lat wskazało, że w ostatnim roku doświadczyło przynajmniej jednej z analizowanych form cyberagresji seksualnej. Zakres obejmował m.in. obraźliwe komentarze ze względu na płeć, nękanie, molestowanie oraz grożenie ujawnieniem materiałów intymnych, odmowę ich usunięcia i tworzenie lub rozpowszechnianie takich materiałów bez zgody osoby przedstawionej[33]. Tak szeroka obecność tych zachowań wymaga zabezpieczeń wbudowanych w zwykłe korzystanie z serwisów.

15 Co dziesiątemu badanemu nastolatkowi grożono ujawnieniem materiałów seksualnych

Według badania NASK obraźliwych komentarzy ze względu na płeć doświadczyło 28,1% badanych, uporczywego śledzenia aktywności online – 24,4%, a molestowania seksualnego w internecie – 19,8%. W usłudze może zatem dochodzić do stopniowego przekraczania granic, zanim pojawi się fotografia lub otwarta groźba[34].

Na grożenie udostępnieniem dotyczących ich materiałów o charakterze seksualnym wskazało 10,6% uczniów. 10% doświadczyło odmowy usunięcia takich materiałów mimo prośby, a 8,9% – tworzenia lub rozpowszechniania seksualnych materiałów wizualnych przedstawiających ich bez zgody. W takich sytuacjach szybka reakcja może ograniczyć rozpowszechnianie materiałów i ryzyko dalszego nękania lub szantażu[35].

Odmowa usunięcia materiału pokazuje szczególnie wyraźnie, dlaczego dziecko potrzebuje interwencji administracji. Zwrócenie się do publikującego już nie wystarczyło. Materiał nadal pozostaje dostępny w usłudze platformy, dlatego jej administracja powinna zapewnić skuteczną drogę zgłoszenia naruszenia prywatności i intymności pokrzywdzonej osoby. Odsyłanie pokrzywdzonego z powrotem do sprawcy może tylko utrwalić przewagę osoby, która dysponuje intymnym materiałem.

Niechciany kontakt powinien dać się zakończyć bez dalszej negocjacji. Blokada musi być łatwa do znalezienia i zrozumienia. Zgłoszenie groźby powinno uwzględniać całą rozmowę, kolejne konta i ryzyko publikacji, nawet jeśli materiał jeszcze nie trafił do publicznego obiegu. Ochrona uruchamiana dopiero po szerokim rozpowszechnieniu materiału przychodzi za późno: nie zatrzymuje ani pierwszej publikacji, ani poprzedzającego ją szantażu.

16 Co dziesiąty badany nastolatek doświadczył co najmniej pięciu rodzajów cyberagresji seksualnej

W badaniu NASK 9,8% uczniów w wieku 14–18 lat zadeklarowało, że w ostatnim roku doświadczyło pięciu lub więcej rodzajów cyberagresji seksualnej. To niemal co dziesiąty uczestnik badania[36].

Obraźliwe komentarze, nękanie, groźby i rozpowszechnianie intymnych materiałów mogą dotyczyć tej samej osoby. Rozpatrywanie każdego zda-

rzenia osobno utrudnia ocenę pełnej skali przemocy.

17 70,7% pokrzywdzonych nikomu nie powiedziało o najbardziej dotkliwym incydencie przemocy seksualnej online

W badaniu „Nastolatki" 28% uczniów deklarowało otrzymanie czyjegoś nagiego lub półnagiego zdjęcia, podczas gdy wiedzę o takim doświadczeniu dziecka wskazywało 7% rodziców. Materiał intymny trafia więc do młodych użytkowników znacznie częściej, niż dostrzegają to dorośli. Platforma powinna zapewniać łatwe ograniczenie otrzymywania takich treści i reagowanie na ich dalsze przesyłanie bez zgody[37].

Możliwość przekazania pliku jednym ruchem nie może przesłaniać praw osoby przedstawionej. Platforma powinna jasno informować, że bezprawne rozpowszechnianie cudzych zdjęć lub nagrań intymnych narusza prawa osoby przedstawionej, oraz zapewniać skuteczną drogę zgłoszenia takiego naruszenia. Dziecko, którego materiał krąży w grupie, nie ma narzędzi do wycofania go z urządzeń kolejnych odbiorców. Tym większe znaczenie ma interwencja w samej usłudze i ograniczanie ponownego udostępniania.

Wśród pokrzywdzonych pytanych o najbardziej dotkliwy incydent 70,7% nie ujawniło go nikomu. Wśród osób, które powiedziały o zdarzeniu, najczęściej jako powiernicy pojawiali się kolega lub koleżanka (49,1%), rodzice lub opiekunowie (23,4%) oraz partner lub partnerka (15,1%). Wielu dorosłych nie dowiaduje się więc o doświadczeniu, które młoda osoba uznała za najbardziej dotkliwe[38].

Szantażysta może wzmacniać przekonanie, że dziecko zostanie obwinione za rozpoczęcie rozmowy lub wysłanie fotografii. Procedura platformy nie może powtarzać tego komunikatu. Wcześniejsza zgoda na wykonanie albo wysłanie zdjęcia nie daje prawa do jego rozpowszechniania, tworzenia przeróbek ani wymuszania przesłania następnych materiałów. Pomoc należy się niezależnie od tego, jak zaczęła się relacja.

18 76,5% pokrzywdzonych nastolatków nie znało tożsamości sprawcy cyberprzemocy seksualnej

W badaniu NASK „Agresja i przemoc seksualna w internecie" 76,5% pokrzywdzonych nie znało tożsamości sprawcy swojego najbardziej dotkliwego doświadczenia. Pytanie zadano uczniom w wieku 14–18 lat, którzy w ostatnim roku doświadczyli co najmniej jednej formy cyberagresji seksualnej[39].

Pokrzywdzony może wskazać konto sprawcy i opisać, co się wydarzyło, nawet jeśli nie wie, kto je prowadzi. Nie należy oczekiwać, że sam ustali tożsamość tej osoby. Próba uzyskania dodatkowych informacji może oznaczać kolejny kontakt z kimś, kogo się obawia. Ustalenie tożsamości sprawcy niekiedy wymaga działań służb, ale platforma może zablokować niechciany kontakt bez czekania na ich wynik.

19 29-latek miał szantażować dziewczęta poniżej 15. roku życia. Wszystko zaczęło się od fałszywych profili

W sierpniu 2025 r. Centralne Biuro Zwalczania Cyberprzestępczości opisało sprawę 29-letniego Polaka zatrzymanego w Niemczech. Według ustaleń przywołanych w komunikacie podejrzany używał fałszywych profili, zdobywał zaufanie dziewcząt poniżej 15. roku życia, a następnie wykorzystywał intymne zdjęcia do szantażu i wymuszania kolejnych materiałów. Opis dotyczył dwóch pokrzywdzonych[40].

Opisany mechanizm pokazuje znaczenie kolejnych etapów kontaktu. Sprawca najpierw staje się osobą, z którą dziecko chce rozmawiać. Później wykorzystuje to, co uzyskał w relacji. Platforma powinna ograniczać niepożądane kontakty z małoletnimi, ułatwiać zakończenie rozmowy i reagować na sygnały wymuszenia. Samo usunięcie profilu po zakończeniu wielomiesięcznej przemocy nie rozstrzyga o skuteczności wcześniejszej ochrony.

Inny komunikat Policji, z Lublina z lutego 2019 r., opisywał szantażowanie trzynastolatki zdjęciami. Mechanizmy, które doprowadziły do pozyskania tych materiałów, były takie jak opisane wyżej. Powracanie podobnego schematu działań w kolejnych latach wymaga reakcji platformy wykraczającej poza jednostkową interwencję. Platformy mają możliwość ucze-

nia systemów ochrony na rozpoznanych nadużyciach[41].

20 69% badanych osiemnastolatków z Polski doświadczyło krzywdy na tle seksualnym w internecie przed osiągnięciem pełnoletności

WeProtect Global Alliance i Economist Impact w badaniu z 2023 r. zapytały osiemnastolatków, czy przed ukończeniem 18 lat doświadczyli w internecie którejś z czterech form krzywdy seksualnej: otrzymywania od dorosłych treści o charakterze seksualnym lub prób rozmowy na takie tematy, nakłaniania do niechcianych czynności seksualnych online, prośby o zachowanie w tajemnicy seksualnej relacji z dorosłym oraz udostępniania ich seksualnych zdjęć lub filmów bez zgody. W polskiej części, obejmującej 500 osób, 69% wskazało co najmniej jedną z analizowanych form; 51% było nakłanianych do niechcianych czynności seksualnych online, a 21% doświadczyło udostępnienia ich seksualnych zdjęć lub filmów bez zgody[42].

W tej samej polskiej części badania wśród osób, którym dorosły – znajomy lub nieznajomy – przesyłał treści seksualne lub próbował rozmawiać z nimi na tematy seksualne, 81% doświadczało tego przez telefon komórkowy, a 58% przez prywatne komunikatory. Działanie sprawcy może więc pozostawać niewidoczne w publicznym profilu dziecka. Ochrona ograniczona do publicznych wpisów pomija ważną drogę kontaktu[43].

21 11% badanych nastolatków spotkało się z dorosłym poznanym w sieci. Co czwarty z nich nikomu o tym nie powiedział

Ochrona kontaktu ma znaczenie także wtedy, gdy relacja przechodzi poza internet. 11% uczniów biorących udział w badaniu NASK spotkało się z dorosłą osobą poznaną w sieci. Wśród nastolatków z takim doświadczeniem 28% nie poinformowało nikogo o planowanym spotkaniu. Te wyniki pokazują, jak ważne są dostęp do zaufanego dorosłego oraz narzędzia pozwalające zakończyć kontakt budzący niepokój[44].

Rodzic nie powinien otrzymywać sprzecznych instrukcji z kilku części tej samej aplikacji. W sprawie dziecka liczy się jedna, spójna droga uzyskania

ochrony.

Spotkanie poza internetem rzadko jest pierwszym krokiem. Zwykle poprzedza je okres budowania zaufania, przeniesienie rozmowy do prywatnego komunikatora i prośba o zachowanie znajomości w tajemnicy. Wszystkie te etapy rozgrywają się w usługach konkretnych platform.

22 1,4 miliona dzieci w wieku 7–14 lat odwiedzało strony z kategorii „Erotyka"

Krzywdząca treść może dotrzeć do dziecka bez jego poszukiwań. Pojawia się w wiadomości, grupie, reklamie albo strumieniu rekomendacji. Znajomy przesyła fragment filmu. Kolejny materiał uruchamia się automatycznie. Ochrona ograniczona do ostrzeżenia przed wpisywaniem określonych haseł nie obejmuje tych dróg. Dostawca odpowiada za to, jak jego usługa otwiera dostęp do takich treści i jak potrafi go zatrzymać.

W badaniu NASK 41% nastolatków potwierdziło przynajmniej jeden kontakt z pornografią w internecie. Wśród respondentów z takim doświadczeniem średni wiek pierwszego kontaktu wynosił 11 lat i 3 miesiące. Spośród osób, które zetknęły się z pornografią, 15% wskazywało oglądanie jej codziennie, a kolejne 18% – przynajmniej raz w tygodniu[45].

Pierwszy kontakt z pornografią w tym wieku oznacza, że zabezpieczenia usług dla dorosłych i aplikacji pośredniczących w dostępie muszą uwzględniać dzieci ze szkoły podstawowej. Platforma nie może czekać, aż użytkownik sam rozpozna treść jako nieodpowiednią i poprawnie ją zgłosi.

Raport „Internet dzieci" wskazuje około 1,4 mln użytkowników w wieku 7–14 lat odwiedzających w analizowanym okresie witryny zaliczone do kategorii „Erotyka". Ta szeroka kategoria opisuje zasięg dostępu do treści erotycznych obejmujących również pornografię. To kolejny sygnał, że same regulaminowe ograniczenia wieku nie zatrzymują kontaktu dzieci z obszarem przeznaczonym dla dorosłych[46].

23 58% rodziców deklaruje kontrolę kontaktu dzieci z pornografią. Potwierdza ją tylko 18% nastolatków

W badaniu NASK 58% rodziców deklarowało, że kontroluje lub sprawdza, czy ich dziecko ogląda pornografię. Taką kontrolę zauważało tylko 18% nastolatków. Wyniki pokazują, że rodzice i dzieci odmiennie oceniają zakres nadzoru[47].

Kontrola rodzicielska działa zwykle tylko w jednej aplikacji, na jednym koncie lub urządzeniu i rzadko sięga do prywatnych wiadomości. Rodzic powinien się o tym dowiedzieć już podczas konfiguracji. Inaczej łatwo uzna, że dziecko jest bezpieczne, i przeoczy niepokojące sygnały albo odłoży rozmowę. Dlatego informacja o włączonej ochronie musi jasno określać jej zasięg i luki.

Potrzebne są też rozwiązania, które nie obciążają dziecka winą za przypadkowy kontakt z treściami nieodpowiednimi do jego wieku. Użytkownik powinien móc szybko przerwać ekspozycję, ograniczyć kolejne rekomendacje i uzyskać zrozumiałą pomoc. Platforma nie może wymagać wielokrotnego odtwarzania materiału po to, by wybrać odpowiednią kategorię naruszenia.

24 22% badanych nastolatków oglądało patostreamy

Patostreamer włącza kamerę, a widzowie oglądają na żywo, jak się upija, bije, wyzywa albo poniża innych. Często robi to na zamówienie publiczności, która płaci za coraz mocniejsze sceny.

Badanie FDDS „Patotreści w internecie” z 2019 r. pokazało, że 37% badanych nastolatków oglądało takie materiały. Wśród odbiorców 43% miało z nimi kontakt co najmniej raz w tygodniu. 73% oglądających wskazywało krótkie fragmenty patostreamów na YouTube. Patostreamy docierają więc do widzów nie tylko w czasie transmisji na żywo. Wycięte z nich krótkie fragmenty z najbardziej drastycznymi scenami są ponownie publikowane, polecane przez algorytmy i udostępniane dalej. Dzięki temu mogą trafić do znacznie większej liczby odbiorców. Także do dzieci, które nigdy nie obejrzałyby całej transmisji[48].

W nowszym badaniu NASK 22% nastolatków deklarowało oglądanie patostreamów. To nadal znacząca grupa odbiorców treści, które przyciągają

widzów właśnie agresją, poniżaniem uczestników i coraz bardziej ryzykownymi zachowaniami. Dążenie do utrzymania zainteresowania odbiorców może skłaniać twórców do eskalowania zachowań agresywnych, poniżających i ryzykownych[49].

25 Publiczne piętnowanie dziewcząt w mediach społecznościowych

W 2025 r. polskie nastolatki poznały nowe słowo: „szon patrol". Ośrodek Analizy Dezinformacji NASK opisał to zjawisko w raporcie za ten rok. Chłopcy zakładali anonimowe konta o nazwach w rodzaju „szon patrol" z dopisaną nazwą miasta lub szkoły. Publikowali na nich zdjęcia dziewcząt zrobione bez ich wiedzy, z komentarzem, że wyglądają „wyzywająco". Na Instagramie pojawiały się też konta z listami profili wskazanych dziewcząt, służące – według analityków – ich piętnowaniu i narażaniu na hejt. Po zgłoszeniach część kont zniknęła, ale inne zostały, choć publikowały takie same treści. Ochrona zależała więc od tego, na które konto trafiła dana skarga. Odrzucona skarga pozostawiała pokrzywdzone osoby bez jednolitej ochrony[50].

W tej samej dokumentacji TikTok usunął niemal wszystkie zgłoszone mu materiały związane z tym zjawiskiem. To ważne ustalenie – platforma może podjąć działanie, kiedy rozpoznaje naruszenie. Niespójność reakcji Instagrama wymaga zatem wyjaśnienia. Dostawca powinien pokazać, jak jego zespoły oceniają użycie zdjęcia, nazwy konta i listy profili w szerszym kontekście nękania.

Ochrona musi działać po polsku. Lokalny język, aluzje, nazwy akcji i sposób użycia wizerunku mogą decydować o sensie publikacji. Pokrzywdzona nie powinna tłumaczyć od podstaw każdemu kolejnemu moderatorowi, dlaczego jej zdjęcie na konkretnym profilu służy publicznemu upokorzeniu.

26 Filtry, lajki i presja idealnego ciała. Dzieci dorastają pod nieustanną oceną wyglądu

Anna Borkowska w publikacji NASK „Pod presją. Internet, media i popkultura a seksualizacja dzieci" opisuje sprowadzanie wartości młodej osoby do atrakcyjności i zewnętrznej oceny. W mediach społecznościowych presja może łączyć się z filtrami, retuszem i publicznym mierze-

niem popularności. Młody człowiek porównuje własne ciało z obrazem starannie wybranym i przetworzonym[51].

W wywiadzie OSE (Ogólnopolska Sieć Edukacyjna) „5 pytań o... presję i seksualizację dzieci w internecie" autorka zwraca uwagę na uczenie się zależności między wyglądem a reakcjami odbiorców. Ten opis stawia przed platformami pytanie o projekt produktu: jakie wzorce ich systemy nagradzają i jak chronią dziecko przed uporczywym ocenianiem ciała[52].

Szczególnie pilnej ochrony wymagają treści zachęcające do głodzenia się, samouszkadzania albo skrajnego podporządkowania ciała cudzej ocenie. Jeśli użytkownik zaznaczy, że nie chce oglądać takich treści – np. wybierając opcję „Nie interesuje mnie to" – platforma powinna trwale przestać mu je podsuwać, nie tylko ten jeden film, lecz także podobne materiały, i nie wracać do nich po kilku dniach.

27 Co czwarty badany nastolatek uczestniczył w internetowym wyzwaniu. Stawką bywa zdrowie i życie

NASK odnotował udział w internetowym wyzwaniu w ostatnim roku u 26% nastolatków, podczas gdy rodzice wskazywali takie doświadczenie u 11% dzieci.

Internetowe wyzwania (challenge) to nagrania, w których uczestnicy wykonują określone zadanie i zachęcają innych do jego powtórzenia. Wiele z nich jest nieszkodliwych, ale część polega na zachowaniach zagrażających zdrowiu[53].

Publikacja NASK i Ministerstwa Cyfryzacji „W sieci wyzwań. Sztuka wychowania w cyfrowym świecie" podkreśla, że o udziale często decydują relacje z rówieśnikami i presja grupy – młody człowiek może podjąć wyzwanie, by nie zostać wykluczonym, zyskać uznanie lub nie wyjść na tchórza. Dlatego tak ważne jest, by dorośli umieli o tym rozmawiać i reagować bez ośmieszania dziecka. Istotna odpowiedzialność spoczywa również na platformach, których systemy rekomendacji mogą zwiększać zasięg niebezpiecznych wyzwań i przyczyniać się do ich szybkiego rozpowszechniania wśród dzieci.

28 2866 potwierdzonych przypadków materiałów przedstawiających seksualne wykorzystywanie dzieci w jednym roku

Krzywda nie kończy się wraz z aktem wykorzystania, który utrwalono na zdjęciu lub nagraniu. Rozpowszechnianie materiału przedstawiającego seksualne wykorzystywanie dziecka odnawia naruszenie jego intymności. Każda kolejna publikacja daje następny dostęp do zapisu przemocy. Dostawca usługi, przez którą materiał krąży, ma obowiązek reagować na zgłoszone naruszenie i usuwać materiał. Powinien też blokować kolejne kopie tego samego zdjęcia lub nagrania, zanim znów trafią do serwisu.

Zespół Dyżurnet.pl, działający w NASK, odnotował w 2025 r. 9298 zgłoszeń dotyczących potencjalnych materiałów przedstawiających seksualne wykorzystywanie dzieci. Analiza potwierdziła 2866 incydentów CSAM, jak określa się tę kategorię treści. W tym samym roku zespół wykazał 63 incydenty szantażu seksualnego wobec małoletnich. To konkretna praca analityczna i interwencyjna prowadzona wobec ujawnionych zagrożeń[54].

29 3848 działań związanych z przekazaniem spraw organom ścigania i międzynarodowej sieci INHOPE

Platformy i instytucje opisują przemoc językiem technicznym – mówią o „materiale", „adresie URL", „koncie" i „incydencie". Takie pojęcia są potrzebne do obsługi zgłoszeń, ale nie oddają tego, co przeżywa dziecko. Dla niego każdy „incydent" oznacza kolejną osobę, która mogła zobaczyć zapis jego krzywdy. Pokrzywdzone dziecko traci kontrolę nad tym zapisem. Usunięcie jednej kopii może przynieść ulgę, ale świadomość, że inne nadal krążą, podtrzymuje poczucie zagrożenia. Ochrona wymaga więc zapobiegania ponownej publikacji tego samego materiału oraz wsparcia osoby, której prawa naruszono.

NASK wskazuje w raporcie Dyżurnet.pl także 3848 działań związanych z przekazywaniem spraw organom ścigania i zespołom INHOPE. Skuteczna interwencja angażuje wiele instytucji i często przekracza granice państw. Ten wysiłek nie zwalnia usługodawców z wykonywania własnej części pracy. Publiczne zespoły nie powinny stale wracać do tego samego rozpoznanego materiału tylko dlatego, że dostawca nie ograniczył jego ponownego pojawiania się w sieci[55].

30 104 282 zgłoszenia stron z materiałami seksualnego wykorzystywania dzieci w wieku 7–10 lat. Wzrost o 65%

Internet Watch Foundation w raporcie za 2023 r. wykazała 104 282 zgłoszenia stron zawierających materiały określane jako „self-generated" z udziałem dzieci w wieku 7–10 lat (o 65% więcej niż w 2022 r.). Termin obejmuje także sytuacje, w których sprawca zdalnie manipuluje dzieckiem, oszukuje je lub szantażuje, aby uzyskać materiał. Brak fizycznej obecności sprawcy nie wyklucza przemocy[56].

To szczególnie ważne wobec popularnego argumentu, że dziecko było bezpieczne, ponieważ pozostawało we własnym pokoju. Urządzenie umożliwia kontakt z osobą, która przejmuje wpływ na zachowanie młodego użytkownika. Ochrona musi obejmować zdalne wymuszenie, presję wywieraną w wiadomościach prywatnych i nakłanianie do wykonywania oraz przesyłania zdjęć lub nagrań o charakterze seksualnym.

Projektując mechanizmy ochrony, platformy muszą uwzględniać również sytuację dziecka, które nie potrafi jeszcze rozpoznać i nazwać wykorzystywania seksualnego albo pozostaje emocjonalnie związane ze sprawcą. Projekt usługi nie może zakładać, że młody użytkownik zawsze poprawnie rozpozna intencje rozmówcy i sam uruchomi wszystkie zabezpieczenia.

31 Najpierw obietnica przynależności, potem szantaż i przemoc. Tak działają sadystyczne grupy internetowe

Dyżurnet.pl w komunikacie z 2 października 2026 r. ostrzega przed grupami dopuszczającymi się sadystycznej przemocy online. Opisuje społeczności wykorzystujące samotność i potrzebę przynależności, a następnie wciągające młode osoby w wymuszenia i przemoc. Status w grupie może zależeć od udokumentowanego udziału w krzywdzących działaniach. Pokrzywdzona osoba może z czasem być nakłaniana do krzywdzenia następnych[57].

Zagrożenie ma wtedy charakter relacyjny i grupowy. Zablokowanie jednego konta może nie zakończyć nacisku, jeśli pozostałe osoby z tej samej społeczności zachowują kontakt. Platforma potrzebuje możliwości

oceny powiązanych zgłoszeń i reakcji na całą rozpoznaną aktywność. Musi jednocześnie chronić dziecko przed odwetem oraz współpracować z właściwymi instytucjami.

Komunikat opisuje zjawisko obserwowane przede wszystkim za granicą. Dyżurnet.pl odnotował jednak również zgłoszenie z Polski.

32 Sprawca przenosi się między aplikacjami. Dziecko nie może uciec przed przemocą

Kontakt może rozpocząć się w serwisie o dużym zasięgu, przejść do prywatnego komunikatora, a materiał trafić do kolejnego miejsca przechowywania. Rodzina widzi jedną historię krzywdy. Dostawcy widzą jej fragmenty objęte własnymi regulaminami. Ten podział nie może pozbawiać pokrzywdzonego skutecznej interwencji.

Platformy muszą sprawnie współpracować z Policją (w tym z Centralnym Biurem Zwalczania Cyberprzestępczości), prokuraturą i sądami, a także z wyspecjalizowanymi zespołami, takimi jak Dyżurnet.pl. Dziecko nie powinno pełnić roli koordynatora postępowania między firmami.

Każdy powrót rozpoznanego materiału jest kolejnym zadaniem ochronnym. Rodzic nie może miesiącami sam szukać kopii i odtwarzać całej historii przy każdej skardze.

33 Co trzeci pokrzywdzony cyberagresją seksualną odczuwał później niepokój podczas korzystania z technologii

Platforma rozpatruje zgłoszenie i przesyła rodzinie decyzję – na przykład, że materiał nie narusza regulaminu albo że usunięto jedną jego kopię. Dla platformy sprawa jest wtedy zamknięta, ale dla rodziny często dopiero się zaczyna. Jeśli krzywdzący materiał nadal krąży, dziecko idzie do szkoły ze świadomością, że koledzy i koleżanki mogli go widzieć. Musi mierzyć się z ich pytaniami, komentarzami i docinkami. Do nauki musi korzystać z telefonu, komputera i komunikatorów, czyli tych samych narzędzi, przez które dociera do niego przemoc i w których może ponownie zobaczyć krzywdzący materiał. Lęk przed kolejną wiadomością czy powiadomieniem może towarzyszyć mu przez cały dzień – w drodze

do szkoły, na lekcjach i wieczorem. Skuteczności reakcji nie można więc oceniać po tym, że zgłoszenie zostało w systemie platformy zamknięte.

W badaniu NASK dotyczącym cyberagresji seksualnej 33,4% pokrzywdzonych wskazywało późniejszy dyskomfort lub niepokój podczas korzystania z technologii cyfrowych; 27,9% czuło się mniej bezpiecznie i komfortowo przy ich używaniu w szkole, a 24,3% ograniczyło korzystanie z technologii; 21,9% zaczęło odnosić się bardziej negatywnie do ich wykorzystywania w szkole[58].

To wymierny opis utraty poczucia bezpieczeństwa. Urządzenie służące do nauki i kontaktu zaczyna kojarzyć się z zagrożeniem. Pokrzywdzony może wycofywać się z aktywności, które pozostałym osobom nadal pomagają uczyć się i utrzymywać relacje. W ten sposób dodatkowy ciężar ponosi właśnie dziecko, którego prawa naruszono. Skuteczna ochrona powinna umożliwiać powrót do bezpiecznego korzystania z usług cyfrowych.

34 Cyberprzemoc nie kończy się po wyłączeniu telefonu. Strach wraca z każdym powiadomieniem

Niepewność jest częścią krzywdy. Dziecko nie wie, kto zachował kopię materiału i kiedy zostanie ona ponownie udostępniona. Sprawdza telefon, choć sama ta czynność może budzić lęk. Zrezygnowanie z aplikacji nie daje pewności, że publikacja przestała krążyć. Potrzebuje informacji o realnych działaniach platformy, a nie jedynie potwierdzenia otrzymania skargi.

Rodzice równocześnie szukają pomocy, rozmawiają ze szkołą i próbują ograniczyć obieg materiału. Każda kolejna odmowa może oznaczać ponowne opisanie sprawy, tłumaczenie jej kontekstu i ustalanie, jak odwołać się od decyzji. Platforma powinna ograniczać ten ciężar przez ciągłość obsługi. Pokrzywdzony nie powinien zaczynać procesu od początku po każdej zmianie osoby lub narzędzia rozpatrującego zgłoszenie.

Równie ważne jest zrozumiałe wyjaśnienie granic interwencji. Jeżeli usunięto konkretną publikację, rodzina powinna wiedzieć, czego dotyczy decyzja i co zrobić w razie powrotu naruszenia. Jeżeli są podstawy do pilnego działania właściwych służb – procedura musi je uwzględniać. Niejasny komunikat zwrotny może skłaniać rodzinę do przekonania, że sprawę zakończono, choć realnie zagrożenie nadal istnieje.

35 55% nastolatków chce ograniczyć korzystanie z telefonu. 31% próbowało bez powodzenia

W badaniu NASK 55% nastolatków widziało potrzebę ograniczenia korzystania z telefonu, a 52% przyznawało, że używa go dłużej, niż zamierzało; 31% próbowało ograniczyć korzystanie bez powodzenia, a 25% odczuwało przymus ponownego sięgnięcia po urządzenie zaraz po jego odłożeniu. Takie deklaracje wymagają reakcji także od dostawców usług walczących o uwagę młodych osób[59].

W tej samej edycji badania 36% uczniów uzyskało wynik wskazujący na wysoki lub bardzo wysoki poziom objawów problematycznego użytkowania internetu w skali E-SAPS18, w tym 5% znalazło się w kategorii bardzo wysokiego nasilenia. To sygnał trudności z korzystaniem z usług cyfrowych, który powinien przekładać się na kontrolę funkcji podtrzymujących aktywność[60].

Na pytanie, czy brak smartfona uczyniłby ich życie nieszczęśliwym, 40% badanych uczniów odpowiedziało twierdząco. Wynik obejmuje odpowiedzi „zdecydowanie tak", „tak" i „raczej tak"[61].

Odpowiedź polegająca na zaleceniu większej samodyscypliny pozostawia dziecko sam na sam z produktem, który przez cały czas zachęca do pozostania na platformie.

Zwykły czas odpoczynku również pozostaje pod presją. NASK odnotował korzystanie z internetu podczas zasypiania u 50% nastolatków, a podczas nauki lub odrabiania lekcji w celach niezwiązanych z nauką – u 45%. Usługi wchodzą więc w momenty wymagające wyciszenia albo skupienia. Domyślne ustawienia powinny wspierać ochronę takich okresów i umożliwiać skuteczne odłożenie aplikacji[62]. Usługi projektowane w sposób zachęcający dzieci do kompulsywnego i nadmiernego korzystania z sieci, w tym mechanizmy nieprzerwanego odtwarzania treści, utrudniające zakończenie sesji, i nagradzanie regularnej aktywności powinny być zakazane.

36 Filtry poprawiają wygląd, ale nie samoocenę. Presja idealnego ciała zaczyna się na ekranie

Filtry i starannie wybierane publikacje tworzą punkt odniesienia dla oceny własnego wyglądu. Liczby reakcji dodatkowo porządkują tę ocenę –

określony obraz zdobywa uwagę, inny pozostaje bez odpowiedzi. To platforma organizuje widoczność tych sygnałów.

Publikacje NASK o seksualizacji i pułapkach sieci opisują znaczenie presji wyglądu, porównywania się i potrzeby akceptacji. Ochrona dziecka wymaga uwzględnienia tego codziennego otoczenia. Nie można poprzestać na usuwaniu materiałów jawnie łamiących regulamin – np. instruujących, jak się głodzić lub okaleczać – jeżeli pozostałe funkcje uporczywie podtrzymują niebezpieczny wzorzec oceny ciała albo kierują ku treściom zachęcającym do szkodliwych zachowań[63].

W brytyjskim „Digital Youth Index 2022" 37% badanych młodych osób zgadzało się, że korzystanie z internetu ma negatywny wpływ na ludzi takich jak one. To głos samych użytkowników o ich cyfrowym otoczeniu – powinien mieć znaczenie w publicznej ocenie usług, podobnie jak skargi rodzin, którym nie udało się uzyskać ochrony[64].

37 22% uczniów zgłaszających przemoc otrzymało tylko obietnicę pomocy. 16% zostało zignorowanych

FDDS w raporcie „Rówieśnicy 2026" pokazała również reakcje na ujawnienie przemocy rówieśniczej. Wśród uczniów, którzy ją zgłosili, 33% wskazało wysłuchanie i próbę pomocy, 22% samą obietnicę pomocy bez dalszego działania, a 16% – zignorowanie zgłoszenia; 39% uznało, że uzyskana pomoc doprowadziła do rozwiązania problemu. Takie doświadczenia wpływają na gotowość do kolejnego proszenia o wsparcie[65].

Inne badanie NASK „Agresja i przemoc seksualna w internecie" pokazuje, jak pokrzywdzeni oceniali pomocność podzielenia się swoim doświadczeniem. Wśród respondentów odpowiadających na to pytanie 27,2% uznało, że niczego to nie zmieniło, a 23,1% oceniło je jako bardzo pomocne[66].

Dziecko potrzebuje dorosłego, który potraktuje je poważnie, wyjaśni kolejne kroki i pozostanie w kontakcie. Potrzebuje też platformy, która zatrzyma naruszenie w usłudze. Te działania powinny postępować równolegle. Jeżeli szkoła obiecuje pomoc, a administracja aplikacji pozostawia treść w obiegu – skuteczność interwencji zostaje ograniczona przez brak działania dostawcy usługi.

Rodzina musi wiedzieć, kto prowadzi sprawę dziecka – kto odpowiada za nią w szkole, kto po stronie platformy i do kogo zwrócić się w razie kolejnego incydentu. W sytuacji zagrożenia zdrowia lub życia liczy się pilna interwencja odpowiednich służb i dostęp do specjalistów.

38 Psycholog pomaga dziecku, ale koszmar trwa. Upokarzające nagranie nadal krąży w sieci

Wsparcie może zmniejszać lęk i pomagać odzyskać poczucie wpływu. Nie zastąpi jednak usunięcia krzywdzącej publikacji, zatrzymania kontaktu sprawcy ani naprawy niebezpiecznej funkcji. Finansowanie pomocy bez egzekwowania tych działań pozostawiałoby rodzinę w sytuacji, w której próbuje dochodzić do równowagi, a usługa nadal dostarcza kolejne naruszenia.

Temat wpływu mediów społecznościowych i algorytmów na zdrowie psychiczne dzieci, w tym na zachowania samobójcze, był przedmiotem posiedzenia sejmowej podkomisji 19 listopada 2025 r. Uczestniczyli w nim m.in. przedstawiciele NASK i organizacji zajmujących się ochroną dzieci. Władze publiczne mają również obowiązek przekładać rozpoznane zagrożenia na działający nadzór i pomoc[67].

Nie można leczyć skutków krzywdy, pozostawiając bez kontroli dalszy obieg materiału, który ją utrwala. Państwo powinno łączyć wsparcie rodziny z rozliczaniem dostawcy za wypełnianie jego obowiązków. Dziecko potrzebuje odzyskać poczucie bezpieczeństwa w codziennym życiu i w aplikacji, z której korzysta. Dopiero te dwa rezultaty razem pozwalają oceniać, czy interwencja przyniosła trwałą poprawę sytuacji.

39 Algorytm układa, co zobaczy dziecko. Platforma odpowiada za to, co mu podsuwa

To platforma układa strumień treści, który widzi dziecko. Wybiera sygnały służące rekomendowaniu, decyduje o kolejności wyświetlania materiałów i ustala domyślne zachowanie aplikacji. Krótkie zatrzymanie przy filmie, reakcja na niego albo ponowne odtworzenie mogą stać się informacją dla systemu. Dostawca powinien sprawdzać, kiedy takie dopasowanie zwiększa zagrożenie dla młodego użytkownika.

Przycisk zgłaszania pojedynczych wpisów to za mało. Problem może

tkwić w ciągu materiałów i sposobie podtrzymywania ekspozycji. Dziecko odrzuca jeden film, lecz dostaje kolejne o podobnym przekazie. System rozpoznaje zainteresowanie tematem, ale nie rozróżnia ciekawości, lęku i bezradnego sprawdzania zagrożenia. Platforma ma obowiązek badać takie sytuacje w ocenie ryzyka.

40 TikTok pod lupą Komisji Europejskiej. Zarzuty dotyczą mechanizmów uzależniających

W wielu aplikacjach kolejny film uruchamia się automatycznie, a strumień treści nie ma końca – po jednym materiale od razu pojawia się następny. Znikają więc naturalne momenty, w których użytkownik mógłby się zatrzymać i zdecydować, czy chce oglądać dalej, takie jak koniec odcinka serialu czy ostatnia strona gazety. Powiadomienia działają podobnie, ale poza aplikacją – dźwięk lub komunikat na ekranie telefonu ściąga dziecko z powrotem, nawet gdy odrabia lekcje albo zasypia. To, jak zaprojektowano autoodtwarzanie, nieskończone przewijanie i powiadomienia, w dużym stopniu decyduje o tym, ile czasu i w jaki sposób dzieci spędzają w aplikacji. Odpowiedzialność za ten projekt ponosi dostawca. To on może np. domyślnie wyłączyć autoodtwarzanie na kontach dzieci, ograniczyć powiadomienia albo wprowadzić przerwy w przewijaniu.

6 lutego 2026 r. Komisja Europejska wstępnie stwierdziła naruszenie DSA przez TikToka w związku z uzależniającą konstrukcją usługi. Wskazała m.in. nieskończone przewijanie, autoodtwarzanie, powiadomienia i silnie spersonalizowane rekomendacje. Oceniła również, że istniejące narzędzia zarządzania czasem i kontroli rodzicielskiej nie wydają się skutecznie ograniczać tych zagrożeń[68].

41 Dziecko ogląda film o samookaleczeniach. Algorytm podsuwa mu kolejne podobne treści

Szczególnej ochrony wymagają użytkownicy trafiający na treści promujące samouszkodzenia, głodówki lub niebezpieczne zachowania. Sygnał, że dziecko nie chce oglądać określonego tematu, musi zmieniać rekomendacje w sposób trwały i zrozumiały.

Wytyczne Komisji Europejskiej dotyczące ochrony małoletnich wskazują znaczenie bezpiecznych systemów rekomendacji, możliwości ich resetowania i ograniczania funkcji podtrzymujących nadmierne korzystanie.

Dają podstawę do pytań o konkretne ustawienia usług dostępnych dla dzieci. Nadzór powinien sprawdzać ich działanie na różnych kontach i w sytuacjach odpowiadających rzeczywistemu korzystaniu[69].

Reset rekomendacji powinien być łatwy do znalezienia. Użytkownik potrzebuje też zrozumiałej informacji, na co wpływa i co stanie się po jego użyciu. Platforma nie może obiecywać kontroli, której efekt znika po kilku kolejnych interakcjach. Szczególnie ważna jest możliwość odcięcia ciągu materiałów, które wiążą się z kryzysem, przemocą albo presją dotyczącą ciała.

Prawo do odpoczynku od aplikacji musi mieć odzwierciedlenie w jej ustawieniach. Bezpieczne konto dziecka powinno ograniczać niepotrzebne powiadomienia, chronić nocny odpoczynek i umożliwiać zakończenie sesji. Rodzic nie powinien musieć przeszukiwać wielu zakładek, by włączyć podstawowe zabezpieczenia, takie jak wyciszenie powiadomień w nocy czy limit czasu korzystania. Na koncie dziecka powinny one działać domyślnie, a ich ustawienia powinny być zebrane w jednym, łatwo dostępnym miejscu.

42 Wyzwiska, seksizm i groźby podczas gry. Wirtualna rozgrywka, prawdziwa przemoc

Gry online tworzą przestrzeń rozmów, grup i publicznej oceny. Dziecko może pozostawać w kontakcie z osobami, których nie zna poza grą, używać czatu głosowego i przenosić relacje do zewnętrznego komunikatora. Zabezpieczenia powinny obejmować te funkcje tak samo poważnie jak profil w serwisie społecznościowym. Samo oznaczenie wieku odpowiedniego dla treści gry nie rozstrzyga o bezpieczeństwie wszystkich kontaktów wokół niej.

NASK w „Pułapkach sieci" opisuje wyzwiska, seksizm, groźby i wykluczanie pojawiające się w niektórych społecznościach graczy. Szczególne znaczenie ma czat głosowy, w którym agresywny komunikat dociera natychmiast. Użytkownik powinien móc szybko wyciszyć kontakt, zgłosić nękanie i uzyskać pomoc[70].

Odpowiedzialność platform obejmuje również narzędzia tworzenia grup, zapraszania do rozmów i przenoszenia kontaktu. Należy jasno pokazywać, kto może kontaktować się z dzieckiem i jak zmienić ten zakres. Zgłoszenie w czasie rozgrywki nie może wymagać rezygnacji z całego

konta i relacji. Pokrzywdzony powinien zachować możliwość bezpiecznego uczestnictwa w grze, a sprawca – utracić narzędzie dalszego ataku.

43 Wirtualne skrzynki, prawdziwe pieniądze. Dzieci wciągane w spiralę kolejnych zakupów

Publikacje „W sieci wyzwań" oraz „Pułapki sieci" zwracają uwagę na lootboxy (wirtualne skrzynki z losowymi nagrodami) oraz inne mechanizmy zachęcające do kolejnych zakupów. Przypomina to grę losową – użytkownik płaci, z napięciem czeka na wynik losowania, a gdy nagroda go rozczaruje, może jednym kliknięciem od razu kupić kolejną skrzynkę. Wobec dzieci wymaga to szczególnej kontroli dostępu, w tym ograniczenia możliwości korzystania z takich mechanizmów, a także nadzoru nad tym, w jaki sposób gra zachęca do zakupów[71].

Wirtualna waluta może utrudniać odczytanie rzeczywistego kosztu zakupu. Mały zakup powtarzany wiele razy staje się znaczącym wydatkiem, a ograniczona czasowo oferta zwiększa presję decyzji. Dostawca powinien podawać cenę w sposób zrozumiały i zapewniać skuteczne ograniczenia wydatków. Zakupy dziecka nie mogą zależeć wyłącznie od tego, czy dorosły dostrzeże każdą drobną transakcję.

Dziecięca potrzeba przynależności nie może być narzędziem wymuszania kolejnej płatności. W społeczności graczy znaczenie mogą mieć wygląd postaci, posiadane dodatki i możliwość udziału w danej aktywności.

Nadzór nad usługą powinien obejmować projekt płatności, zasady przyznawania losowych nagród i sposób prezentowania ofert małoletnim. Potrzebna jest również kontrola reklam i promocji kierujących dziecko do zewnętrznych miejsc zakupu. Podział na grę, sklep i komunikator nie może rozmywać odpowiedzialności za mechanizm, który korzysta z ich połączenia.

44 Ulubiony influencer sprzedaje, dziecko wierzy. Reklama ukryta pod pozorem przyjaźni

Przekaz handlowy może pojawić się w filmie ulubionego twórcy, relacji z gry albo rekomendacji produktu. Dziecko potrzebuje zrozumiałej informacji, że za publikacją stoi interes finansowy. NASK w przewodniku „Masz wpływ" opisuje odpowiedzialność twórców za publikowane treści i relacje z odbiorcami[72].

Oznaczenie ma być widoczne w miejscu kontaktu z przekazem, także w krótkim fragmencie i ponownym udostępnieniu. Dziecko nie powinno szukać tej informacji w długim opisie poza ekranem filmu. To platforma decyduje, jak wyglądają publikacje w jej serwisie. Może więc wprowadzić jednolite, dobrze widoczne oznaczenie treści reklamowych – np. etykietę „reklama" lub „współpraca płatna" wyświetlaną bezpośrednio na filmie – i wymagać od twórców, by z niej korzystali.

DSA zakazuje objętym tym obowiązkiem platformom prezentowania małoletnim reklam opartych na profilowaniu z wykorzystaniem ich danych, gdy dostawca wie z wystarczającą pewnością, że odbiorca jest małoletni. Przepis ma być wykonywany w praktyce. Nadzór powinien badać, jak platforma rozpoznaje sytuację użytkownika i zapobiega obchodzeniu ochrony[73].

45 63% badanych nastolatków nie znało pojęcia deepfake, choć 70% korzystało z narzędzi AI

Popularność materiału nie potwierdza jego wiarygodności. W badaniu Sorousha Vosoughiego, Deba Roya i Sinana Arala opublikowanym w „Science" w 2018 r. fałszywe wiadomości w analizowanych przekazach na Twitterze rozchodziły się szerzej i szybciej niż prawdziwe. Badanie pokazuje szerszy problem rozpowszechniania fałszywych informacji, oszustw i treści budujących presję grup[74].

Intensywny obieg groźby, plotki o rówieśniku lub informacji o rzekomym wyzwaniu może sprawiać wrażenie, że ktoś już sprawdził ich wiarygodność. Dla młodego użytkownika popularność przekazu może więc zastępować jego weryfikację. Platformy organizujące ten obieg powinny ograniczać manipulacje i jasno oznaczać treści, które promują. Nie można oczekiwać, że dziecko samo sprawdzi wiarygodność wszystkiego, co podsuwa mu serwis.

NASK w raporcie „Nastolatki” odnotował, że 63% badanych nie znało pojęcia deepfake, podczas gdy 70% korzystało z narzędzi sztucznej inteligencji. Nowe możliwości tworzenia i przekształcania treści są więc już częścią codzienności. Wiedza o mechanizmach manipulacji nie nadąża u wszystkich za samą dostępnością narzędzi[75].

Dostawca generatora i platforma rozpowszechniania materiałów muszą jasno informować o charakterze syntetycznych treści, przeciwdziałać podszywaniu się i ograniczać naruszanie praw dziecka. Oznaczenie materiału ma być widoczne tam, gdzie użytkownik go ogląda, a nie schowane gdzieś w regulaminie.

46 Dziecko zwierza się chatbotowi z najskrytszych problemów. Jego sekrety i bezpieczeństwo trafiają w ręce technologicznych gigantów

Coraz więcej dzieci korzysta z chatbotów, czyli programów opartych na sztucznej inteligencji, które prowadzą z użytkownikiem rozmowę jak człowiek. Są dostępne jako osobne aplikacje, ale także wbudowane w komunikatory i serwisy społecznościowe. Dla młodej osoby taki chatbot może stać się powiernikiem – dziecko pyta go o relacje z rówieśnikami i pierwsze związki, o swój wygląd i ciało, dzieli się trudnymi emocjami, samotnością, smutkiem, a nawet myślami o samookaleczeniu. Odpowiedź brzmiąca pewnie może zdobyć zaufanie młodego użytkownika nawet wtedy, gdy jest błędna. NASK w „Pułapkach sieci” opisuje ryzyko nadmiernego polegania na odpowiedziach AI i przekazywania takim narzędziom zbyt wielu danych[76].

Produkt dostępny dla dziecka musi uwzględniać rozmowy o przemocy, szantażu i zagrożeniu zdrowia. Potrzebne są zabezpieczenia przed udzielaniem szkodliwych instrukcji oraz kierowanie do odpowiedniej pomocy. Platforma musi sprawdzać działanie zabezpieczeń także w języku polskim, w wypowiedziach potocznych i w sytuacji, gdy młoda osoba nie nazywa kryzysu wprost. Dziecko w kryzysie może posługiwać się żartem, slangiem lub niedopowiedzeniami, dlatego zabezpieczenia powinny rozpoznawać również takie sygnały.

Brakuje również wyjaśnienia, co dzieje się z treścią rozmowy, jak długo jest przechowywana i jakie możliwości kontroli ma użytkownik. Firma udostępniająca narzędzie zyskuje zapis bardzo wrażliwych informacji

o konkretnej osobie. Nie może go gromadzić, przechowywać ani wykorzystywać, np. do trenowania modeli czy personalizacji treści, bez jasnych, zrozumiałych dla dziecka zasad i odpowiednich zabezpieczeń.

Ochrona obejmuje możliwość przerwania rozmowy i zwrócenia się do człowieka. Interfejs nie powinien utrudniać zakończenia rozmowy z chatbotem – np. przez zachęcanie, by użytkownik „jeszcze został" – ani wzmacniać przekonania, że narzędzie zastępuje pomoc bliskich lub specjalisty. Państwo ma wymagać od platform oceny takich ryzyk przed szerokim udostępnieniem produktu dzieciom. Rozwój usługi musi iść w parze ze sprawdzaniem jej wpływu na bezpieczeństwo użytkownika.

47 Wizerunek dziecka służy nowym formom przemocy

Do stworzenia fałszywego materiału intymnego może wystarczyć zwykła fotografia. Sprawca nie potrzebuje autentycznego nagiego zdjęcia dziecka. Narzędzie generatywne pozwala przetworzyć wizerunek, a platforma ułatwia dotarcie z nim do odbiorców. Szkoda dotyczy rozpoznawalnej osoby – to ona mierzy się z komentarzami, wstydem i groźbą dalszego rozpowszechniania materiału.

W styczniu 2026 r. NASK informował o zgłoszeniach do Dyżurnet.pl dotyczących seksualizujących i pornograficznych materiałów, które miał generować Grok, narzędzie firmy xAI. Komunikat obejmował również materiały przedstawiające seksualne wykorzystywanie dzieci. Po krytyce xAI ogłosiło ograniczenia technologiczne i dostęp do części funkcji przez konta płatne[77].

Przypadek stawia zasadnicze pytanie o moment uruchomienia ochrony. Zabezpieczenia powinny działać przed udostępnieniem funkcji, która może naruszać intymność dziecka. Dostawca generatora ma sprawdzać przewidywalne nadużycia i wykazywać skuteczność blokad. Platformy nie mogą czekać na publiczny skandal, by wykonać podstawową pracę nad bezpieczeństwem produktu.

48 28% badanych nastolatków doświadczyło co najmniej jednej formy cyberataku

NASK odnotował, że 28% nastolatków doświadczyło co najmniej jednej z analizowanych form cyberataku, podczas gdy rodzice wskazywali takie doświadczenie u 13% dzieci. Wśród zagrożeń raport opisuje włamania na konta i inne nadużycia cyfrowe. Utrata kontroli nad profilem może otwierać dostęp do prywatnych rozmów i umożliwiać podszywanie się pod jego właściciela[78].

Należy zapewniać łatwe zabezpieczenie konta i szybką drogę odzyskania dostępu. Uwierzytelnianie wieloskładnikowe, ostrzeżenia o podejrzanym logowaniu oraz kontrola aktywnych sesji powinny być zrozumiałe dla młodego użytkownika. Gdy konto dziecka zostało już przejęte, najważniejsze jest szybkie zablokowanie wiadomości i publikacji wysyłanych w jego imieniu przez osobę, która przejęła profil.

„Masz wpływ" zwraca uwagę na znaczenie haseł, dodatkowego uwierzytelniania i zarządzania dostępami. W przypadku dziecka narzędzia te muszą uwzględniać możliwość utraty telefonu i potrzebę wsparcia opiekuna. Procedura odzyskiwania konta nie może sama ujawniać nadmiernych danych ani stawiać wymagań, których młody użytkownik nie jest w stanie spełnić[79].

49 Intymne zdjęcia dzieci krążą po internecie latami

Usługa Take It Down, prowadzona przez National Center for Missing & Exploited Children, pozwala utworzyć cyfrowy skrót intymnego zdjęcia lub filmu wykonanego przed ukończeniem 18. roku życia. Uczestniczące platformy wykorzystują go do wykrywania kopii w publicznych lub nieszyfrowanych częściach swoich usług. Sam obraz pozostaje na urządzeniu osoby korzystającej z narzędzia[80].

Takie rozwiązanie pokazuje możliwość technicznego wsparcia ochrony przed dalszym obiegiem materiału. Rodzina potrzebuje jednak jasnej informacji o jego zasięgu i pomocy w użyciu. Dziecko ma prawo do ochrony także wtedy, gdy nie zna nazwy specjalistycznego narzędzia.

50 Nawet 81% zgłoszeń zewnętrznych odrzuconych lub bez odpowiedzi. Tak platformy reagują na sygnały o dezinformacji

Brak skutecznej reakcji platformy pozwala krzywdzie trwać. W sprawie dziecka zwłoka może oznaczać kolejne udostępnienia, następną groźbę i rozszerzenie kręgu odbiorców. Przyjęty formularz jest dopiero początkiem. Ochrona wymaga działania w usłudze oraz zrozumiałej informacji, co zostało zatrzymane i co stanie się dalej.

Raporty OAD NASK pokazują poważne problemy ze sprawnym funkcjonowaniem procedur. W kwartalnych zestawieniach za 2025 r. od 57% do 81% zgłoszeń zewnętrznych pochodzących od obywateli i instytucji w monitoringu dezinformacji zaliczono do odrzuconych. Kategoria obejmowała również brak odpowiedzi w przyjętym okresie obserwacji. Dane te dotyczą dezinformacji, a nie krzywdzenia dzieci. Pokazują jednak, jak w praktyce działają kanały zgłoszeniowe platform – te same, z których korzysta rodzic albo dziecko, prosząc o usunięcie krzywdzącej treści[81].

51 76% zgłoszeń dezinformacji odrzuconych lub pozostawionych bez działania w pierwszym półroczu 2026 roku

W całym monitoringu OAD za 2025 r. odnotowano 46 511 zgłoszonych materiałów. 12% usunięto, 68% objęto moderacją, a 20% zaliczono do odrzuconych. Moderacja mogła obejmować inne działania niż usunięcie. Takie wyniki wymagają pytań o to, czy zastosowany środek odpowiadał rozpoznanemu zagrożeniu i czy skutek był wystarczający[82].

W pierwszym półroczu 2026 r. OAD zgłosił 65 220 treści i kont zakwalifikowanych w monitoringu jako dezinformacyjne; 4380 usunięto, 11 270 objęto moderacją, a 49 570 zaliczono do odrzuconych lub pozostawionych bez działania. Ostatnia grupa stanowiła 76% zgłoszeń. Sama możliwość wysłania sygnału nie przesądzała zatem o skutecznej reakcji dostawcy[83].

Te dane dotyczą monitoringu dezinformacji. Pokazują jednak konkretny problem organizacyjny platform – co dzieje się po otrzymaniu udokumentowanego sygnału. W ochronie dzieci zasadnicze znaczenie mają osobno opisane sprawy nękania i naruszania intymności. W obu obszarach administracja musi umieć rozpoznać kontekst, uzasadnić decyzję

i zastosować działanie odpowiednie do zagrożenia.

52 Platforma X odrzuciła niemal 79% zgłoszeń dotyczących dezinformacji. Instagram i TikTok też pod lupą

W zestawieniu OAD za pierwsze półrocze 2026 r. na platformie X do odrzuconych zaliczono 47 464 spośród 60 132 zgłoszeń, czyli 78,9%. Na Instagramie było to 97 ze 156 zgłoszeń, czyli 62,2%, a na TikToku 488 z 1109, czyli 44%. Każda z tych firm powinna odpowiadać za własny wynik i wyjaśniać przyczyny decyzji dotyczących udokumentowanych zgłoszeń[84].

Duże różnice w odsetku odrzuconych zgłoszeń między X, Instagramem i TikTokiem mogą pokazywać, że skuteczność reagowania nie jest cechą internetu w ogóle, lecz wynika z decyzji konkretnej firmy. Należy zbadać, w jakim stopniu te decyzje wynikają z charakteru zgłaszanych treści, liczby i kompetencji moderatorów, znajomości polskiego języka i kontekstu oraz sposobu działania procedur odwoławczych. Użytkownik nie powinien otrzymywać słabszej ochrony dlatego, że jego relacje społeczne przeniosły się do aplikacji, w której procedura działa gorzej.

W sprawach dzieci raport OAD opisuje szczególnie wymowny przypadek kont na Instagramie związanych z piętnowaniem dziewcząt. Część zgłoszeń odrzucono mimo podobieństwa materiałów. W tej samej dokumentacji odnotowano skuteczną reakcję TikToka wobec niemal wszystkich zgłoszonych mu treści tego rodzaju. To podstawa żądania wyjaśnień i naprawy praktyki moderacji[85].

Jeżeli skuteczna reakcja jest możliwa w jednej usłudze, rodzina ma prawo pytać, dlaczego zawodzi w drugiej. Dostawca powinien ujawniać, jak rozpoznaje powtarzalne nękanie i co robi po wykryciu błędnej odmowy.

53 Facebook odrzucił 1194 zgłoszenia dezinformacji. Co trzeci alarm bez reakcji platformy

W pierwszym półroczu 2026 r. Facebook usunął 2150 materiałów zgłoszonych jako dezinformacja, 37 objął innymi działaniami moderacyjnymi, a 1194 zgłoszenia odrzucił. Tak wynika z raportu OAD NASK. Oznacza to,

że ponad jedna trzecia zgłoszeń nie doprowadziła do interwencji. Wyniki pokazują, dlaczego platformy powinny jasno informować, jak reagują na zgłoszenia i jakie działania podejmują wobec wskazanych treści[86].

BIBLIOGRAFIA

ABW, ABW zatrzymała kolejną osobę. Zarzut przygotowywania zamachu terrorystycznego, komunikat z września 2026

ABW, Zatrzymanie dwóch 16-latków. Sprawa dotyczy radykalizacji i ekstremizmu, komunikat z 18.09.2026

Bigaj M. i in., Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie, 2025

Borkowska A., Pod presją. Internet, media i popkultura a seksualizacja dzieci, OSE NASK, 2026

CBZC, Poszukiwany dwoma listami gończymi mężczyzna zatrzymany na terenie Niemiec, 29.08.2025

Dyżurnet.pl, Gdy to przemoc staje się celem. Rosnące zagrożenie dla młodych użytkowników internetu, 2.10.2026

Dyżurnet.pl, NASK, Raport 2025, 2026

FDDS, Rówieśnicy. Raport 2026 o przemocy rówieśniczej, 2026

FDDS, RPO, Patotreści w internecie. Raport o problemie, 2019

Gańko K., Pułapki sieci. Sieć pułapek, NASK, 2026

Internet Watch Foundation, Annual Report 2023

Komisja Europejska, wstępne ustalenia dotyczące uzależniającej konstrukcji TikToka, 6.02.2026

Komisja Europejska, wytyczne dotyczące ochrony małoletnich na podstawie art. 28 ust. 4 DSA, C/2025/5519

NASK, Agresja i przemoc seksualna w internecie, 2025

NASK, Dyżurnet.pl alarmuje – Grok „rozbiera” także dzieci, 15.01.2026

NASK, Masz wpływ. Przewodnik po cyberbezpieczeństwie dla twórców cyfrowych, 2026

NASK, Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców, 2025

NASK, Ministerstwo Cyfryzacji, W sieci wyzwań. Sztuka wychowania w cyfrowym świecie, 2025

Nominet, UK's youth faced with sharpening digital inequalities and alarming levels of online abuse, Digital Youth Index 2022

OAD NASK, Reakcja platform społecznościowych na zgłoszenia w 2025 roku, 2026

OAD NASK, Reakcja platform społecznościowych na zgłoszenia w I półroczu 2026 roku, 2026

OSE / NASK, 5 pytań o... presję i seksualizację dzieci w internecie, wywiad z Anną Borkowską

Policja, Bili, kopali i przypalali papierosem. Policjanci z Gdańska zatrzymali trzy osoby, które znęcały się nad 15-latkiem, 21.04.2026

Policja, Lublin. Szantażował 13-latkę zdjęciami, 8.02.2019

Radio Poznań, Nagranie z nożem i groźba „krwawego piątku". Alarm w szkole w Krobi, 11.10.2026, aktualizacja 12.10.2026

Rowicka M., Bujalski M., Brzdąc w sieci – zjawisko korzystania z urządzeń mobilnych przez dzieci w wieku 0–6 lat, Raport z badania, 2020

Shah B., Kaushik P., Copycat crimes: exploring the intersection of violent media, technology, and digital culture on criminal behavior, "Discover Global Society" 2025, vol. 3(111)

Vosoughi S., Roy D., Aral S., The spread of true and false news online, "Science" 2018, vol. 359(6380)

Ybarra M.L., Mitchell K.J., Oppenheim J.K., Violent Media in Childhood and Seriously Violent Behavior in Adolescence and Young Adulthood, "Journal of Adolescent Health" 2022, vol. 71(3)

Youth Endowment Fund, Children, Violence and Vulnerability 2024, komunikat o przemocy w mediach społecznościowych

WeProtect Global Alliance / Economist Impact, Estimates of childhood exposure to online sexual harms and their risk factors. A study of childhood experiences of 18-year-olds in four European countries. Poland country profile, 2023

WHO/Europe, One in six school-aged children experiences cyberbullying, finds new WHO/Europe study, 27.03.2024

PRZYPISY KOŃCOWE

1 NASK, Nastolatki. Raport z ogólnopolskiego badania uczniów i rodziców, 2025, s. 70–79. Źródło.

2 NASK, Agresja i przemoc seksualna w internecie, 2025, s. 36–38; najbardziej dotkliwy incydent; adresaci ujawnienia wśród osób, które je zadeklarowały. Źródło.

3 M. Bigaj i in., Internet dzieci. Raport z monitoringu obecności dzieci i młodzieży w internecie, 2025, s. 51–54 numeracji drukowanej; aktywni użytkownicy aplikacji na smartfonach w wieku 7–12 lat. Źródło.

4 K. Gańko, Pułapki sieci. Sieć pułapek, NASK, 2026, części I–II i IV. Źródło.

5 OAD NASK, Reakcja platform społecznościowych na zgłoszenia w 2025 roku, 2026, s. 145–146. Źródło.

6 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065, akt o usługach cyfrowych, art. 34–35. Tekst rozporządzenia.

7 M. Bigaj i in., Internet dzieci..., s. 51–54 numeracji drukowanej; aktywni użytkownicy aplikacji na smartfonach w wieku 7–12 lat. Źródło.

8 FDDS, Rówieśnicy. Raport 2026 o przemocy rówieśniczej, 2026, s. 23; korzystanie z aplikacji i stron w ostatnim roku wśród uczestników badania. Źródło.

9 FDDS, Rówieśnicy..., s. 24; uczestnicy w wieku 10–12 lat. Źródło.

10 M. Rowicka, M. Bujalski, Brzdąc w sieci – zjawisko korzystania z urządzeń mobilnych przez dzieci w wieku 0–6 lat, Raport z badania, 2020, s. 2 i 52–54. Źródło.

11 NASK, Nastolatki..., s. 27–30. Źródło.

12 NASK, Nastolatki..., s. 32–36 i 49–50; deklaracje uczniów, edycja badania 2024. Źródło.

13 M. Bigaj i in., Internet dzieci..., s. 30 numeracji drukowanej; Mediapanel, IV kwartał 2024, internauci w wieku 7–14 lat. Źródło.

14 M. Bigaj i in., Internet dzieci..., s. 56–57 numeracji drukowanej; korzystanie z aplikacji internetowych w dni powszednie w grupach wieku 7–12 i 13–18 lat. Źródło.

15 NASK, Nastolatki..., s. 47–50; średnie liczby kont oraz czas korzystania z mediów społecznościowych. Źródło.

16 NASK, Nastolatki..., s. 112–116; odpowiedzi uczniów i rodziców. Źródło.

17 Europejska Rada Ochrony Danych, Oświadczenie 1/2025 w sprawie zapewnienia wieku, 11.02.2025, część 2. Źródło.

18 Rozporządzenie (UE) 2016/679, RODO, art. 8 w związku z art. 6 ust. 1 lit. a; regulaminowe ograniczenia dostępu stanowią odrębną kwestię. RODO.

19 NASK, Nastolatki..., s. 70–75; deklarowane doświadczenia przemocy internetowej. Źródło.

20 NASK, Nastolatki..., s. 73–74, wykres 27; baza: 1439 uczniów z doświadczeniem przemocy internetowej. Około 24% stanowi sumę trzech zaokrąglonych kategorii odpowiedzi: 7% + 7% + 10%. Źródło.

21 FDDS, Rówieśnicy..., s. 25; uczestnicy badania w wieku 10–17 lat. Źródło.

22 FDDS, Rówieśnicy..., s. 27 i 30; cztery formy cyberprzemocy oraz osobny pomiar cyberbullyingu. Źródło.

23 WHO/Europe, One in six school-aged children experiences cyberbullying, finds new WHO/Europe study, 27.03.2024; HBSC 2021/2022. Źródło.

24 Policja, Bili, kopali i przypalali papierosem. Policjanci z Gdańska zatrzymali trzy osoby, które znęcały się nad 15-latkiem, 21.04.2026. Komunikat.

25 Youth Endowment Fund, Children, Violence and Vulnerability 2024, komunikat o przemocy w mediach społecznościowych; 10 tys. osób w wieku 13–17 lat, Anglia i Walia. Źródło.

26 M.L. Ybarra, K.J. Mitchell, J.K. Oppenheim, Violent Media in Childhood and Seriously Violent Behavior in Adolescence and Young Adulthood, "Journal of Adolescent Health" 2022, vol. 71(3), s. 285–292, DOI: 10.1016/j.jadohealth.2022.03.003. Artykuł.

27 B. Shah, P. Kaushik, Copycat crimes: exploring the intersection of violent media, technology, and digital culture on criminal behavior, “Discover Global Society” 2025, vol. 3(111); artykuł przeglądowy. Artykuł.

28 ABW, Zatrzymanie dwóch 16-latków. Sprawa dotyczy radykalizacji i ekstremizmu, komunikat z 18.09.2026. Komunikat.

29 ABW, ABW zatrzymała kolejną osobę. Zarzut przygotowywania zamachu terrorystycznego, komunikat z września 2026; stan postępowania opisany przez Agencję. Komunikat.

30 Radio Poznań, Nagranie z nożem i groźba „krwawego piątku”. Alarm w szkole w Krobi, 11.10.2026, aktualizacja 12.10.2026; wypowiedź rzeczniczki Policji Moniki Curyk. Źródło.

31 NASK, Nastolatki..., s. 70–79. Źródło.

32 FDDS, Rówieśnicy..., s. 35; powody niezgłoszenia przemocy wśród uczniów świadomych jej wystąpienia, którzy nie zgłosili zdarzenia. Źródło.

33 NASK, Agresja i przemoc..., s. 27–29, wykresy 5–6. Źródło.

34 NASK, Agresja i przemoc..., s. 27–29; wykres 6. Źródło.

35 NASK, Agresja i przemoc..., s. 29; 10,6% i 8,9% jako dopełnienia odpowiedzi „nigdy” na wykresie 6. Źródło.

36 NASK, Agresja i przemoc..., s. 27–28, wykres 5; 9,8% ogółu badanych zadeklarowało pięć lub więcej rodzajów cyberagresji seksualnej w ostatnim roku. Źródło.

37 NASK, Nastolatki...., s. 85–87; otrzymywanie nagich lub półnagich zdjęć w deklaracjach uczniów i rodziców. Źródło.

38 NASK, Agresja i przemoc..., s. 36–38; najbardziej dotkliwy incydent; adresaci ujawnienia wśród osób, które je zadeklarowały. Źródło.

39 NASK, Agresja i przemoc..., s. 33–34, wykres 9; pytanie o tożsamość sprawcy najbardziej dotkliwego doświadczenia wśród osób, które w ostatnim roku doświadczyły cyberagresji seksualnej. Źródło.

40 CBZC, Poszukiwany dwoma listami gończymi mężczyzna zatrzymany na terenie Niemiec, 29.08.2025. Komunikat.

41 Policja, Lublin. Szantażował 13-latkę zdjęciami, 8.02.2019; opis stanu sprawy w dniu komunikatu. Komunikat.

42 WeProtect Global Alliance / Economist Impact, Estimates of childhood exposure to online sexual harms and their risk factors. A study of childhood experiences of 18-year-olds in four European countries. Poland country profile, 2023, s. 1–2; 500 osiemnastolatków w Polsce, doświadczenia sprzed pełnoletności. Źródło.

43 WeProtect / Economist Impact, Estimates of childhood exposure..., s. 2; urządzenia i kanały otrzymywania seksualnych treści lub rozmów od wskazanej kategorii osób. Źródło.

44 NASK, Nastolatki..., s. 81–83; spotkania z dorosłymi poznanymi online; ujawnianie planowanego spotkania wśród osób, które się spotkały. Źródło.

45 NASK, Nastolatki..., s. 101–104; wiek i częstotliwość dotyczą osób, które deklarowały kontakt z pornografią. Źródło.

46 M. Bigaj i in., Internet dzieci..., s. 38–39 numeracji drukowanej; kategoria „Erotyka", Mediapanel, IV kwartał 2024. Źródło.

47 NASK, Nastolatki..., s. 108; wykres 48, sumy odpowiedzi twierdzących: rodzice 58%, uczniowie 18%. Źródło.

48 FDDS, RPO, Patotreści w internecie. Raport o problemie, 2019, s. 18–23; częstotliwość i formy wśród oglądających. Źródło.

49 NASK, Nastolatki..., s. 90–94; kontakt z patostreamami. Źródło.

50 OAD NASK, Reakcja platform społecznościowych na zgłoszenia w 2025 roku, s. 145–146. Źródło.

51 A. Borkowska, Pod presją. Internet, media i popkultura a seksualizacja dzieci, OSE NASK, 2026, s. 43–59. Źródło.

52 OSE / NASK, 5 pytań o... presję i seksualizację dzieci w internecie, wywiad z Anną Borkowską. Wywiad.

53 NASK, Nastolatki..., s. 95–99; udział w wyzwaniach internetowych w ostatnim roku. Źródło.

54 Dyżurnet.pl, NASK, Raport 2025, 2026, s. 15–18 i 22–23; zgłoszenia oraz potwierdzone incydenty. Źródło.

55 Dyżurnet.pl, NASK, Raport 2025, s. 22–23; działania dotyczące współpracy z organami ścigania i INHOPE. Źródło.

56 Internet Watch Foundation, Annual Report 2023, część „Self-generated" child sex abuse, grupa 7–10 lat; liczba zgłoszeń stron, nieunikalnych ofiar. Źródło.

57 Dyżurnet.pl, Gdy to przemoc staje się celem. Rosnące zagrożenie dla młodych użytkowników internetu, 2.10.2026. Komunikat.

58 NASK, Agresja i przemoc..., s. 39–40, wykres 14. Źródło.

59 NASK, Nastolatki..., s. 127–129; deklaracje w podskali tolerancja E-SAPS18. Źródło.

60 NASK, Nastolatki..., , s. 125–127; wysoki i bardzo wysoki poziom objawów PUI w skali E-SAPS18. Źródło.

61 NASK, Nastolatki..., s. 131–132, wykres 63; wszyscy uczniowie, N = 3665; suma odpowiedzi twierdzących na pytanie o skutki braku smartfona. Źródło.

62 NASK, Nastolatki..., s. 59–63; korzystanie z internetu równolegle z innymi czynnościami. Źródło.

63 A. Borkowska, Pod presją..., rozdz. 4 i 6; K. Gańko, Pułapki sieci..., rozdz. 13. Pod presją; Pułapki sieci.

64 Nominet, UK's youth faced with sharpening digital inequalities and alarming levels of online abuse, Digital Youth Index 2022, komunikat i wyniki badania; Wielka Brytania, ocena negatywnego wpływu korzystania z internetu na „osoby takie jak respondent". Źródło.

65 FDDS, Rówieśnicy..., s. 35–37; reakcje na zgłoszenie przemocy rówieśniczej, nie wyłącznie internetowej. Źródło.

66 NASK, Agresja i przemoc..., s. 39, wykres 13; odpowiedzi na pytanie o pomocność podzielenia się doświadczeniem cyfrowej przemocy seksualnej. Wskaźnik nie jest oceną wyłącznie profesjonalnej pomocy. Źródło.

67 Sejm RP, Podkomisja stała do spraw sztucznej inteligencji i przejrzystości algorytmów, posiedzenie nr 14, 19.11.2025; porządek obrad i wykaz uczestników. Zapis posiedzenia.

68 Komisja Europejska, wstępne ustalenia dotyczące uzależniającej konstrukcji TikToka, 6.02.2026. Komunikat.

69 Komisja Europejska, wytyczne dotyczące ochrony małoletnich na podstawie art. 28 ust. 4 DSA, C/2025/5519, w szczególności część 6.5. Wytyczne.

70 K. Gańko, Pułapki sieci..., 2026, s. 41–43; społeczności graczy i czaty głosowe. Źródło.

71 NASK, Ministerstwo Cyfryzacji, W sieci wyzwań. Sztuka wychowania w cyfrowym świecie, 2025, s. 150–158; K. Gańko, Pułapki sieci..., s. 42. W sieci wyzwań; Pułapki sieci.

72 NASK, Masz wpływ. Przewodnik po cyberbezpieczeństwie dla twórców cyfrowych, 2026, s. 9–28; odpowiedzialność twórcy i konsekwencje publikacji. Źródło.

73 Akt o usługach cyfrowych, art. 28 ust. 2–3; zakres zakazu i warunek wystarczającej pewności co do małoletności odbiorcy. Tekst rozporządzenia.

74 S. Vosoughi, D. Roy, S. Aral, The spread of true and false news online, "Science" 2018, vol. 359(6380), s. 1146–1151, DOI: 10.1126/science.aap9559; dane Twittera z lat 2006–2017. Artykuł.

75 NASK, Nastolatki..., s. 136–139 i 145–149; znajomość pojęcia deepfake i korzystanie z narzędzi AI. Źródło.

76 K. Gańko, Pułapki sieci..., s. 47–49; narzędzia AI, wiarygodność odpowiedzi i ochrona danych. Źródło.

77 NASK, Dyżurnet.pl alarmuje – Grok „rozbiera" także dzieci, 15.01.2026. Komunikat.

78 NASK, Nastolatki..., s. 67–69; doświadczenia cyberataków w deklaracjach uczniów i rodziców. Źródło.

79 NASK, Masz wpływ..., s. 44–50. Źródło.

80 National Center for Missing & Exploited Children, Take It Down, opis usługi i często zadawane pytania. Dokumentacja.

81 OAD NASK, Reakcja platform społecznościowych na zgłoszenia w 2025 roku, s. 13–15 i 26; zgłoszenia zewnętrzne w kwartalnych zestawieniach. Źródło.

82 OAD NASK, Reakcja platform społecznościowych na zgłoszenia w 2025 roku, s. 23 i 26; wszystkie materiały w monitoringu. Źródło.

83 OAD NASK, Reakcja platform społecznościowych na zgłoszenia w I półroczu 2026 roku, 2026, s. 34–37 i 42–44. Raport.

84 OAD NASK, Reakcja platform społecznościowych na zgłoszenia w I półroczu 2026 roku, s. 42–44; zgłoszenia dezinformacji, różne liczebności dla usług. Raport.

85 OAD NASK, Reakcja platform społecznościowych na zgłoszenia w 2025 roku, s. 145–146. Źródło.

86 OAD NASK, Reakcja platform społecznościowych na zgłoszenia w I półroczu 2026 roku, s. 36 i 43; zgłoszenia dezinformacji dotyczące Facebooka. Raport.