



Ministerstwo Cyfryzacji

Sekretarz Stanu
Michał Gramatyka

BM.WP.057.70.2025
Warszawa, 12 maja 2025 r.

**Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP**

Dot. pisma z 16 kwietnia br. Pośła na Sejm RP Pani Olgii Ewy Semeniuk - Patkowskiej w sprawie ochrony dzieci przed cyberprzemocą (interpelacja nr 9219)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania.

Ad 1) Czy planowane są programy prewencyjne i edukacyjne dla szkół dotyczące bezpieczeństwa w sieci?

Już obecnie Ministerstwo Cyfryzacji wraz z NASK – Państwowym Instytutem Badawczym realizuje szereg inicjatyw, programów i akcji edukacyjno-informacyjnych, które mają na celu zwiększyć bezpieczeństwo dzieci w internecie. W NASK prowadzone są projekty o charakterze edukacyjnym i szkoleniowym na rzecz bezpieczeństwa użytkowników internetu oraz podnoszenia poziomu świadomości i kompetencji cyfrowych. W ramach Działu Profilaktyki Cyberzagrożeń podejmowane są działania związane z kształtowaniem świadomości społecznej w zakresie bezpieczeństwa w sieci dzieci i młodzieży poprzez m.in. prowadzenie warsztatów, lekcji oraz szkoleń, organizacji konferencji, organizacji ogólnopolskich obchodów Dnia Bezpiecznego Internetu (DBI), opracowywania narzędzi edukacyjnych, realizacji społecznych kampanii medialnych. Wśród podejmowanych tematów znajdują się, m.in.: cyberprzemoc i hejt, wizerunek w sieci, ślad cyfrowy, prywatność, higiena cyfrowa, cyfrowy dobrostan, socjotechnika, nielegalne i szkodliwe treści w internecie, dezinformacja, edukacja medialna. Więcej informacji na ten temat dostępnych jest pod adresem www.cyberprofilaktyka.pl. Obok tego w roku szkolnym 2024/2025 trwa cykl comiesięcznych lekcji online dot. zagrożeń w mediach społecznościowych, dedykowanych uczniom szkół podstawowych, które prowadzone są przez specjalistów z Działu Profilaktyki Cyberzagrożeń NASK. Również inne polskie instytucje – w tym Urząd Komunikacji Elektronicznej oraz Urząd Ochrony Danych Osobowych – prowadzą kampanie edukujące dzieci na temat szeroko rozumianej cyberhigieny. Prezes UKE od 2017 r. prowadzi kampanię „Klikam z głową”, której celem jest promowanie bezpiecznego korzystania z internetu i urządzeń telekomunikacyjnych wśród uczniów. W trakcie zajęć porusza się tematy niebezpiecznych zjawisk związanych z korzystaniem z sieci, patostreamingu, uzależnienia od internetu i portali społecznościowych, sextingu, cyberprzemocy, phishingu wraz z poradami jak sobie z nimi radzić.

Ponadto, Ministerstwo Cyfryzacji we współpracy z NASK zaprojektowało Ogólnopolską Sieć Edukacyjną (OSE), czyli publiczną sieć telekomunikacyjną obejmującą szkoły podstawowe i ponadpodstawowe, gwarantującą im dostęp do szybkiego, bezpłatnego i bezpiecznego internetu. Sieć została uruchomiona, aby wspomagać proces kształcenia w placówkach edukacyjnych, podnosić poziom cyfrowych kompetencji uczniów i kadry pedagogicznej, dostosować proces dydaktyczny do wymagań współczesnego świata, a także promować zasady higieny cyfrowej i bezpiecznego korzystania z technologii cyfrowych, w tym do bezpiecznego poruszania się w wirtualnej rzeczywistości, jej rozumienia i właściwego interpretowania napotkanych tam treści. Ponadto, w ramach OSE dostępne jest repozytorium cyfrowych treści edukacyjnych - zawierające materiały

edukacyjne i kursy dla dzieci oraz nauczycieli, mogące również stanowić podstawę scenariusza zajęć, przygotowane przez Ministerstwo Cyfryzacji we współpracy z NASK. Dostępne one są w internecie na stronie: [OSE it-szkoła](#) i dotyczą różnych tematów cyfrowych, z wyszczególnieniem cyberbezpieczeństwa i higieny cyfrowej. Również na stronie [Bezpieczni w sieci](#) dostępne są bezpłatne materiały dedykowane pedagogom oraz uczniom klas 7-8 szkół podstawowych, które podzielone są na moduły edukacyjne, np. cyberprzemoc czy prywatność w cyfrowym świecie. Ministerstwo przygotowało również dla nauczycieli materiały Cyberlekcji i Cyberlekcji 3.0, które znaleźć można na stronie Ministerstwa Cyfryzacji¹. Zawarte są tam materiały dotyczące cyberbezpieczeństwa dedykowane prowadzeniu zajęć dla dzieci szkół podstawowych w różnym wieku, jak i dla starszych dzieci uczęszczających do szkół ponadpodstawowych.

Ad 2) Jakie środki techniczne i legislacyjne podejmowane są w celu blokowania treści nękających dzieci w mediach społecznościowych?

W NASK od 2005 r. funkcjonuje Zespół Dyżurnet.pl, jedyny w Polsce zespół reagujący na nielegalne i szkodliwe treści w internecie, który w ramach swojej działalności, na podstawie Ustawy o krajowym systemie cyberbezpieczeństwa, przyjmuje zgłoszenia dotyczące dystrybucji materiałów przedstawiających seksualne wykorzystywanie dzieci.

Zespół Dyżurnet.pl od 2005 r. realizuje strategię Komisji Europejskiej Better Internet for Children, współtworząc Polskie Centrum Programu Safer Internet (PCPSI) [saferinternet.pl](#). Tworzą je: NASK (koordynator PCPSI) oraz Fundacja Dajemy Dzieciom Siłę. Strategia wdrożona w większości krajów europejskich ([www.betterinternetforkids.eu](#)) ma na celu promowanie bezpiecznego korzystania z internetu i nowych technologii oraz wsparcie reagowania w przypadku zagrożeń online dotyczących najmłodszych.

Dzięki współpracy z wybranymi serwisami internetowymi i portalami społecznościowymi, zespół Dyżurnet.pl działa jako trusted flagger, czyli zaufany podmiot sygnalizujący w ramach tych usług. Zgłoszenia dotyczące bezpieczeństwa dzieci i młodzieży przekazywane przez takie podmioty, są traktowane przez usługodawców priorytetowo.

Ponadto w 2024 r. Dyżurnet.pl zwrócił uwagę na zjawisko dystrybucji treści NCII tzn. materiałów intymnych udostępnianych bez zgody (NCII od ang. Non-consensual Intimate Images). Stanowią one jeden z elementów zjawiska przemocy seksualnej opartej na materiałach wizualnych. To wszelkie materiały, na których utrwalono wizerunek osoby w kontekście intymnym – przedstawiające jej nagość lub uwieczniające ją w sytuacji seksualnej, które zostały (lub istnieje ryzyko, że zostaną) udostępnione bez zgody. Materiały NCII mogą być pozyskane na skutek szantażu na tle seksualnym – gdy w zamian za niedostępność materiałów sprawca chce otrzymać korzyści (albo finansowe albo w postaci kolejnych materiałów). Źródłem może być także grooming, czyli sytuacja, w której dorosły sprawca nawiązuje z dzieckiem relację o podłożu erotycznym. Zdarza się również, że dziecku oferowane są korzyści (pieniądze, prezenty) w zamian za wysłanie intymnych zdjęć. W związku z tym powstały inicjatywy, które pomagają odnaleźć i usunąć takie treści - jest to serwis Take it Down, stworzony przez amerykański hotline NCMEC przeznaczony dla osób poniżej 18. roku życia. Istnieje także StopNCII18 organizacji SWGfL – bliźniaczy serwis, przeznaczony dla osób dorosłych. Narzędzia te umożliwiają odnalezienie i wyeliminowanie niechcianych materiałów z wielu miejsc jednocześnie, bez konieczności kontaktowania się z administratorami kolejnych platform społecznościowych. W 2024 r. Dyżurnet.pl w porozumieniu ze wspomnianymi organizacjami NCMEC oraz SWGfL opracowywał polskojęzyczną wersję serwisu grupującego obecne rozwiązania i przeznaczonego dla polskojęzycznych użytkowników.

¹ <https://www.gov.pl/web/baza-wiedzy/materiały-do-cyberlekcji> oraz <https://www.gov.pl/web/baza-wiedzy/materiały-do-cyberlekcji-30>.

W odniesieniu do platform internetowych i mediów społecznościowych należy zwrócić uwagę na unijne rozporządzenie - Akt o usługach cyfrowych (DSA – Digital Services Act), którego przepisy weszły w życie 17 lutego 2024 r. Zgodnie z DSA dostawcy platform internetowych dostępnych dla małoletnich zobowiązani są do wprowadzenia odpowiednich i proporcjonalnych środków, aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług. Obok tego Komisja Europejska uprawniona jest do wydania odpowiednich wytycznych dotyczących stosowania tych środków, zapewniających ochronę dzieci, jak i poszanowanie ochrony prywatności. Ponadto na podstawie przepisów DSA największe platformy internetowe, zwane VLOP (Very Large Online Platforms), objęte są dodatkowym zakresem obowiązków, do których należą m.in. weryfikacja wieku użytkowników oraz analiza wpływu treści szkodliwych na małoletnich. Wielkie platformy internetowe obecnie już usuwają zgłoszenia kierowane z Dyżurnet.pl.

Ponadto, pod kątem dochodzenia odpowiedzialności platform internetowych względem publikowanych treści należy wspomnieć o pracach nad projektem ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie, które toczą się w Ministerstwie Cyfryzacji. Projekt ustawy stanowi wynik pracy grupy roboczej, w skład której wchodziłi przedstawiciele instytucji publicznych, sektora akademickiego oraz organizacji zajmujących się ochroną dzieci. Grupa poprzez dyskusję zmierzała do przygotowania rekomendacji w zakresie zasadności wprowadzenia regulacji chroniących małoletnich przed szkodliwymi treściami w internecie, w tym: określenia zakresu definicji treści szkodliwych; wskazania podmiotów zobowiązanych do odpowiednich działań w tym aspekcie; przeanalizowania optymalnych rozwiązań technicznych w zakresie weryfikacji wieku. Projekt ustawy przewiduje zwiększenie odpowiedzialności dostawców usług świadczonych drogą elektroniczną za publikowane na ich portalach treści, w tym poprzez wprowadzenie wymogu weryfikacji wieku.

Ad 3) Czy powstanie ogólnopolski system zgłaszania i reagowania na przypadki cyberprzemocy wśród nieletnich?

Ministerstwo na bieżąco analizuje potrzeby osób małoletnich w zakresie ich bezpieczeństwa w internecie. Obecnie w Ministerstwie Cyfryzacji nie trwają prace nad systemem zgłaszania i reagowania na przypadku cyberprzemocy wśród nieletnich. W obowiązującym stanie prawnym w przypadku wystąpienia nękania małoletnich w internecie, osobie poszkodowanej przysługuje prawo zgłoszenia treści do usługodawcy, w którego usłudze doszło do naruszenia, jak również możliwość poinformowania o danym czynie zespołu Dyżurnet.pl, poprzez wypełnienia formularza na stronie: <https://dyzurnet.pl/zglos-nielegalne-tresci/>.

Niektóre akty internetowej agresji naruszają prawo i są uznawane za przestępstwo lub wykroczenie, a tym samym mogą zostać zgłoszone na policję, do prokuratury lub do sądu. Co do zasady ściganie sprawcy cyberprzemocy następuje po złożeniu wniosku przez osobę pokrzywdzoną. Z tego powodu ewentualne prace w zakresie systemu zgłaszania i reagowania na przypadku cyberprzemocy wymagają ścisłej współpracy z Ministerstwem Sprawiedliwości.

Trzeba także zwrócić uwagę, że już obecnie możliwe jest zgłaszanie nielegalnych treści występujących w sieci za pomocą aplikacji mObywatel. Zgłaszane mogą być m.in cyberataki czy oszustwa, ale też niepokojące zachowania wobec dzieci, w tym materiały seksualnego wykorzystywania dzieci. Funkcja „Nielegalne treści” została wprowadzona w ramach usługi „Bezpiecznie w sieci”. Umożliwia użytkownikom aplikacji zgłaszanie niepokojących materiałów, które następnie są analizowane przez ekspertów z zespołu Dyżurnet.pl działającego w NASK, a w razie potrzeby przekazywane odpowiednim służbom w Polsce i za granicą. Dzięki aplikacji mObywatel zgłoszenie można także wystać

anonimowo. Pomimo, że jest ono przesyłane z mObywatela, żadne dane użytkownika nie są przekazywane wraz ze zgłoszeniem. Nie ma to jednak żadnego wpływu na zainteresowanie zgłoszeniem ze strony ekspertów Dyżurnet.pl – bez względu na to, czy zgłoszenie będzie anonimowe, czy nie, wszystkie sprawy będą traktowane tak samo poważnie. Więcej o usłudze można przeczytać na dedykowanej stronie [mObywatel](#).

Obok tego, jak wspomniano powyżej, Polskie Centrum Programu Safer Internet realizuje działania edukacyjne i uświadamiające, podnoszące bezpieczeństwo dzieci i młodzieży w internecie, jak również działania pomocowe polegające na reagowaniu na nielegalne treści w internecie oraz udziela wsparcia poprzez telefony zaufania 116 111 oraz 800 100 100 (prowadzone przez Fundację Dajemy Dzieciom Siłę). Centrum na co dzień współpracuje z Komitetem Konsultacyjnym złożonym z firm i instytucji działających na rzecz bezpieczeństwa dzieci online bądź związanych z obszarem dostępu do usług cyfrowych oraz z młodzieżowym panelem doradczym.

Z wyrazami szacunku

Michał Gramatyka
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych