Ministerstwo
Cyfryzacji

Sekretarz Stanu
Michał Gramatyka

BM.WP.057.230.2025
Warszawa, 05 stycznia 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 9 grudnia br. Posłów na Sejm RP Pani Moniki Rosy oraz Pana Pawła Bliźniuka w sprawie funkcjonowania platformy Kick.com oraz niewystarczających mechanizmów ochrony małoletnich przed treściami szkodliwymi (interpelacja nr 14041)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłów pytania.

Ad 1) Czy Ministerstwo dostrzega narastający problem obecności treści patologicznych, przemocowych i wulgarnych na platformie Kick.com oraz ich wpływu na małoletnich?

Ministerstwo Cyfryzacji monitoruje kwestie związane z ryzykami dla bezpieczeństwa małoletnich w internecie. Ochrona małoletnich przed zagrożeniami w sieci ma dla Ministerstwa szczególne znaczenie. W odpowiedzi na te zidentyfikowane zagrożenia podejmowany jest szereg działań, które mają na celu poprawę sytuacji dzieci w internecie, w tym zmniejszenie dostępności do treści dla nich szkodliwych. Działania, takie jak przywołane w interpelacji dane NASK i Dyżurnet.pl pochodzące z wykonywanych przez te instytucje badań i funkcji, finansowane są między innymi z dotacji przekazywanych do NASK z Ministerstwa Cyfryzacji.

Jednym z zadań realizowanych przez NASK, a zainicjonowanym w 2018 r. przez Ministerstwo Cyfryzacji, jest Ogólnopolska Sieć Edukacyjna (OSE). Jest to publiczna sieć telekomunikacyjna obejmująca szkoły podstawowe i ponadpodstawowe, gwarantująca szkołom dostęp do szybkiego, bezpłatnego i bezpiecznego internetu. OSE zawiera również wiele treści edukacyjnych, w tym scenariusze lekcji dla nauczycieli o cyberzagrożeniach. W ramach OSE realizowany jest projekt edukacyjny adresowany do nauczycieli oraz uczniów klas 7–8 szkół podstawowych i ponadpodstawowych „Bezpieczni w sieci", którego celem jest wspieranie pedagogów, a także młodzieży w podnoszeniu kompetencji cyfrowych z zakresu bezpieczeństwa w sieci. Ponadto w ramach programu OSE IT szkoła przygotowano scenariusze lekcji dla nauczycieli, dotyczące cyberprzemocy, z jaką mogą zetknąć się dzieci i młodzież, a każdym roku szkolnym trwające cykle cykl comiesięcznych lekcji online dedykowanych uczniom szkół podstawowych, które prowadzone były przez specjalistów z Działu Profilaktyki Cyberzagrożeń NASK.

Ministerstwo Cyfryzacji na bieżąco więc zapoznaje się z badaniami i raportami, w tym zwłaszcza wykonywanymi przez NASK, dotyczącymi osób małoletnich, ich zachowania w internecie i ryzyk z tym związanych. Podejmowane przez Ministerstwo oraz NASK działania edukacyjno-informacyjne stanowią, obok prac legislacyjnych, jedną z form odpowiedzi na to ryzyko zwłaszcza w zakresie budowania świadomości wśród dzieci co do zagrożeń związanych z internetem i sposobów radzenia sobie z nimi.

Wykorzystanie programu Ogólnopolskiej Sieci Edukacyjnej stanowi najlepszy sposób na edukację dzieci, umożliwiając zarówno nauczycielom, jak i dzieciom i ich opiekunom dostęp do różnych materiałów edukacyjnych, jak i dotarcie do jak najszerszej liczby małoletnich – uczniów szkół. Z tego powodu Ministerstwo Cyfryzacji we współpracy z NASK utrzymuje portal it-szkola.edu.pl, udostępnia także materiały na stronach bezpieczniwsieci.edu.pl, oraz gov.pl. NASK prowadzi także portal Cyberprofilaktyka NASK,

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

w ramach którego dostępne są poradniki i publikacje dla rodziców i nauczycieli, jak i możliwość zorganizowania szkoleń dla dzieci, rodziców czy nauczycieli, o których wspomniano wcześniej.

Ministerstwo dostrzega więc zwiększające się problemy wpływu treści szkodliwych dostępnych online na małoletnich. Zapoznaniu się z tym problemem, w tym zakresem, źródłami i sposobami ograniczenia treści szkodliwych służyły także prace i spotkania grupy roboczej ds. ochrony małoletnich w internecie, powołanej w 2024 r. przy Ministerstwie Cyfryzacji. Z uczestnikami grupy roboczej konsultowane były założenia projektowanej ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie. Członkowie grupy roboczej zajmujący się na co dzień kwestią treści szkodliwych – przedstawiciele sektora akademickiego, organizacji pozarządowych oraz instytucji publicznych przedstawiali swoje doświadczenia w tym temacie i możliwe kierunki ograniczenia skutków tego dostępu.

Ad 2) Czy Ministerstwo prowadzi lub planuje prowadzić monitorowanie treści publikowanych na Kick. com, w szczególności pod kątem ich zgodności z polskim prawem oraz zagrożeń dla bezpieczeństwa cyfrowego dzieci?

Ministerstwo Cyfryzacji prowadziło prace nad nowelizacją ustawy o świadczeniu usług drogą elektroniczną (dnia 21 listopada 2025 r. ustawa została uchwalona przez Sejm, aktualny status prac legislacyjnych na stronie Sejmu), mającą na celu umożliwienie pełnego stosowania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), dalej jako „DSA", w Polsce. Więcej informacji na ten temat zawiera odpowiedź na pytanie nr 4.

Wzmocnienie ochrony małoletnich ma również na celu procedowany projekt ustawy o ochronie małoletnich przed dostępem do treści pornograficznych w internecie. Zgodnie z projektem, podmioty, w których usługach świadczonych drogą elektroniczną (np. platformy społecznościowe, strony internetowe) znajdują się treści pornograficzne - zostaną zobowiązane do weryfikacji wieku, czyli jednoznacznego stwierdzenia pełnoletniości użytkownika. Projekt przewiduje wprowadzenie rejestru nazw domen zawierających treści pornograficzne, do których dostęp nie jest zabezpieczony weryfikacją wieku. Dostęp do domen wpisanych do rejestru będzie blokowany przez przedsiębiorców telekomunikacyjnych. Projekt ustawy został poddany ponownym konsultacjom publicznym we wrześniu 2025 r. i wkrótce zostanie przekazany do następnego etapu procesu legislacyjnego.

Ponadto, w ramach Naukowej i Akademickiej Sieci Komputerowej funkcjonuje Dyżurnet.pl, czyli zespół ekspertów, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa NASK-PIB został wskazany jako jeden z Zespołów Reagowania na Incydenty Komputerowe tzw. CSIRT.

NASK-PIB prowadzi szkolenia dla dzieci i młodzieży dotyczące patostreamingu. W roku szkolnym 2024/2025 przeprowadzono cykl comiesięcznych lekcji online dedykowanych uczniom szkół podstawowych, które były prowadzone przez specjalistów z Działu Profilaktyki Cyberzagrożeń NASK. Jednym z 10 tematów były treści szkodliwe z uwzględnieniem patotreści. Dostępne materiały edukacyjne online można odnaleźć na stronie Ministerstwa Cyfryzacji oraz na stronie Zintegrowanej Platformy Edukacyjnej.

Eksperci z NASK-PIB przygotowali dostępne materiały edukacyjne dotyczące patostreamingu m.in.:

- gotowy scenariusz lekcji pt. „Co oglądamy w rozbitym lustrze? Królowa Śniegu i patostreamy”- dostępny bezpłatnie na platformie OSE IT Szkoła, animacja, i broszura,
- poradnik dla nauczycieli: „Szkodliwe treści w internecie”,
- poradnik dla rodziców: „Szkodliwe treści w internecie: nie akceptuję, reaguję”.

Patostreamy i inne szkodliwe treści w internecie w komunikacji:

- https://it-szkola.edu.pl/news,art,484;
- https://it-szkola.edu.pl/news,art,357;
- https://it-szkola.edu.pl/news,art,361;
- https://it-szkola.edu.pl/news,art,424;
- https://ose.gov.pl/aktualnosci/wpis/bezpieczni-w-sieci-z-ose-patostreamy;
- https://ose.gov.pl/aktualnosci/wpis/badz-z-innej-bajki-o-cyberzagrozeniachinaczej;
- https://ose.gov.pl/aktualnosci/wpis/temat-lekcji-szkodliwe-tresci-w-internecie.

W ramach kontynuacji projektu Cyberlekcje - Cyberlekcje 3.0, na lata 2025 - 2026 zaplanowano szereg szkoleń dla kadry pedagogicznej i osób zarządzających placówkami oświatowymi w całej Polsce, lekcje online dla uczniów szkół podstawowych i ponadpodstawowych, lekcje pokazowe dla uczniów oraz szkolenia dla nauczycieli i rodziców w placówkach oświatowych. Opracowane zostaną także nowe scenariusze lekcji, odpowiadające na coraz to nowe wyzwania cyfrowego świata. Więcej informacji będzie można odnaleźć na stronie Cyberprofilaktyki NASK.

Ad 3) Czy Ministerstwo analizuje możliwość wprowadzenia obowiązku stosowania przez platformy takie jak Kick skutecznych mechanizmów weryfikacji wieku użytkowników oraz ograniczania dostępu do treści szkodliwych dla małoletnich?

W pierwszej kolejności wskazać należy na przepisy unijnego Aktu o usługach cyfrowych, w którym określono obowiązki platform internetowych. Przepisy tego aktu przewidują m.in. obowiązek wdrożenia przez platformy internetowe odpowiednich i proporcjonalnych środków zapewniających wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych usług. W przypadku największych platform – wskazanych przez Komisję Europejską - przewidziano bardziej rygorystyczne obowiązki, w tym stosowanie narzędzi weryfikacji wieku i kontroli rodzicielskiej. Komisja Europejska prowadzi postępowania przeciwko tym platformom, które nie wywiązują się ze swoich obowiązków zapewnienia bezpieczeństwa małoletnim.

Zwracamy przy tym uwagę, że odgórne wprowadzenie obowiązku restrykcyjnego weryfikowania wieku w celu uniemożliwienia dostępu do szeroko rozumianych treści szkodliwych dzieciom – oznaczałoby w praktyce konieczność weryfikowania większości użytkowników mediów społecznościowych, w odróżnieniu od osób korzystających wyłącznie z platform umożliwiających dostęp do treści pornograficznych. Wobec takiej zmiany w wykorzystywaniu internetu przez jego użytkowników, konieczne jest wyważenie dwóch praw podstawowych – ochrony prywatności z ochroną interesu najmłodszych, w celu wypracowania proporcjonalnego rozwiązania.

Ponadto informuję, że Komisja Europejska opracowuje metodę weryfikacji wieku, z której będą mogły korzystać platformy internetowe. Metoda ma być przyjazna dla użytkownika i jednocześnie chronić jego prywatność. Projekt ten znajduje się w fazie pilotażowej, w trakcie której oprogramowanie do weryfikacji wieku będzie testowane i dalej dostosowywane we współpracy z państwami członkowskimi, platformami internetowymi i użytkownikami końcowymi. Projekt dotyczący weryfikacji wieku ma zapewnić metodę umożliwiającą użytkownikom potwierdzenie ukończenia 18 lat w przypadku dostępu do

ograniczonych treści dla dorosłych, takich jak pornografia dziecięca, bez ujawniania żadnych innych danych osobowych[1].

Dodatkowo należy wskazać, że projektowana ustawa o ochronie małoletnich przed dostępem do treści pornograficznych w internecie również przewiduje objęcie mechanizmem weryfikacji wieku platformy, na których dostępne są treści pornograficzne.

Ad 4) Czy prowadzone są prace nad instrumentami prawnymi umożliwiającymi skuteczniejsze reagowanie na przypadki patostreamingu, w tym obowiązku niezwłocznego usuwania treści zagrażających bezpieczeństwu małoletnich?

Jednym z elementów nowelizacji ustawy o świadczeniu usług drogą elektroniczną stanowiącej wdrożenie DSA jest wprowadzenie procedury wydawania nakazów podjęcia działań przeciwko nielegalnym treściom polegających na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich. Wniosek o wydanie takiego nakazu będzie mógł złożyć do Prezesa Urzędu Komunikacji Elektronicznej lub Przewodniczącego Krajowej Rady Radiofonii i Telewizji (w zakresie treści występujących w usłudze świadczonej przez platformę udostępniania wideo w rozumieniu art. 4 pkt 22a ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji) prokurator, Policja, organ Krajowej Administracji Skarbowej, usługobiorca lub uprawniony z tytułu praw autorskich i praw pokrewnych.

Co istotne, wniosek może dotyczyć wyłącznie treści, których rozpowszechnianie może wyczerpywać znamiona określonych czynów zabronionych (a także nawołujących do popełnienia takich czynów). Wśród wymienionych w art. 11a ust. 1 pkt 1 nowelizowanej ustawy czynów zabronionych znalazły się między innymi następujące czyny obejmujące treści szkodliwe dla małoletnich:

- art. 119 § 1 Kodeksu karnego, który dotyczy stosowania przemocy lub groźby karalnej ze względu na rasę, pochodzenie narodowe lub etniczne, wyznanie bądź bezwyznaniowość i przynależność polityczną. Może obejmować groźby i nękanie w mediach społecznościowych lub innych platformach internetowych;
- art. 151 Kodeksu karnego, który obejmuje namowę lub pomoc w doprowadzeniu do samobójstwa. Może obejmować cyberbullying, namawianie do samobójstwa w ramach platform społecznościowych, co jest szczególnie niebezpieczne w odniesieniu do młodych użytkowników sieci;
- art. 156a Kodeksu karnego, który dotyczy nakłaniania innej osoby do spowodowania u niej ciężkiego uszczerbku na zdrowiu;
- art. 190 § 1 Kodeksu karnego, który dotyczy stosowania groźby karalnej, tj. popełnienia przestępstwa na szkodę osoby lub jej bliskich. W kontekście możliwości popełnienia tego przestępstwa online będzie to obejmowało wiadomości umieszczane w ramach portali społecznościowych;
- art. 190a § 2 Kodeksu karnego, który obejmuje wykorzystanie wizerunku pokrzywdzonego, tak jakby uczynił to on sam w swoim imieniu, przez co wyrządza jej szkodę majątkową lub osobistą;
- art. 191a § 1 Kodeksu karnego, który obejmuje utrwalanie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody;
- art. 200 § 3 i 5 Kodeksu karnego, który dotyczy prezentowania małoletniemu poniżej lat 15 treści pornograficznych albo rozpowszechniania treści

[1] https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint

pornograficznych w sposób umożliwiający takiemu małoletniemu zapoznanie się z nimi;

- art. 200a Kodeksu karnego, który dotyczy nawiązywania kontaktu z małoletnim poniżej 15 lat, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej, w celu popełnienia przestępstwa seksualnego. Obejmuje on grooming, czyli nawiązywanie kontaktu z dziećmi przez internet w celu wykorzystania seksualnego;
- art. 200b Kodeksu karnego, który dotyczy publicznego propagowania lub pochwalania zachowań o charakterze pedofilskim. Obejmuje on publikowanie treści pedofilskich;
- art. 202 § 1, 3–4c Kodeksu karnego, który dotyczy publicznego prezentowania, produkcji, rozpowszechniania, przechowywania treści pornograficznych, zwłaszcza z udziałem małoletnich. W kontekście możliwości popełnienia tego przestępstwa obejmuje on dystrybucję pornografii dziecięcej przez internet, przechowywanie takich treści na serwerach;
- art. 256 § 1–2 Kodeksu karnego, który dotyczy przestępstw związanych z propagowaniem totalitarnych ideologii (nazizmu, komunizmu, faszyzmu lub innego ustroju totalitarnego) oraz nawoływaniem do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość. Obejmuje on treści propagujące totalitaryzm w internecie, zachęcanie do aktów przemocy, może obejmować tworzenie i udostępnianie plików cyfrowych (np. zdjęć, filmów, dokumentów) zawierających takie treści;
- art. 257 Kodeksu karnego, który dotyczy publicznego znieważenia grupy ludności albo osoby lub naruszenia nietykalności cielesnej osoby z powodu przynależności narodowej, etnicznej, rasowej, wyznaniowej. Obejmuje on mowę nienawiści w mediach społecznościowych.

Wprowadzenie powyższej procedury da realne narzędzia do walki z nielegalnymi treściami przy jednoczesnym zachowaniu transparentności postępowania. Przyjęto następujące terminy na wydanie stosownej decyzji:

- 2 dni – gdy wniosek składa Policja lub prokurator,
- 7 dni – gdy wniosek składają pozostałe podmioty, w tym użytkownik,
- 21 dni – w sprawach szczególnie skomplikowanych.

W motywie 71 DSA podkreślono, iż dostawcy platform internetowych, z których korzystają małoletni, powinni wprowadzić odpowiednie i proporcjonalne środki w celu ochrony małoletnich, na przykład poprzez domyślne, w stosownych przypadkach, projektowanie swoich interfejsów internetowych lub ich części z zachowaniem najwyższego poziomu prywatności, bezpieczeństwa i ochrony małoletnich, a także poprzez przyjmowanie norm ochrony małoletnich lub stosowanie kodeksów postępowania służących ochronie małoletnich. Powinni oni uwzględniać najlepsze praktyki i dostępne wytyczne, takie jak te zawarte w komunikacie Komisji pt. „Cyfrowa dekada dla dzieci i młodzieży: nowa europejska strategia na rzecz lepszego internetu dla dzieci” (BIK+)”. Z kolei w motywie 81 wskazano, że przy ocenie rodzajów ryzyka w odniesieniu do praw dziecka dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni przeanalizować na przykład, w jakim stopniu projekt i funkcjonowanie danej usługi są łatwo zrozumiałe dla małoletnich, a także w jaki sposób – poprzez świadczoną przez nich usługę – małoletni mogą zetknąć się z treściami, które mogą mieć szkodliwy wpływ na ich zdrowie oraz rozwój fizyczny, psychiczny i moralny. Takie ryzyko może powstać na przykład w związku z projektem interfejsów

internetowych, które umyślnie lub nieumyślnie wykorzystują słabe strony i niedoświadczenie małoletnich lub które mogą powodować zachowania nałogowe.

W stosunku do bardzo dużych platform (VLOP) i wyszukiwarek internetowych (VLOSE) rolę głównego regulatora pełni Komisja Europejska. KE odpowiada również za wyznaczenie tych podmiotów oraz posiada wyłączne uprawnienia w zakresie nadzorowania i egzekwowania obowiązków określonych w rozdziale III sekcja 5 DSA, tj. obowiązków mających zastosowanie wyłącznie do VLOP i VLOSE.

Na podstawie przepisów opisanych w sekcji 5 DSA (art. 33–43) VLOP oraz VLOSE mają dodatkowy zakres obowiązków, do których należą m.in.: wdrożenie mechanizmów oceny ryzyka, stosowanie – gdy jest to zasadne – weryfikacji wieku użytkowników, a także dokonywanie analiz dotyczących wpływu treści szkodliwych na małoletnich.

Szczególnie należy zwrócić uwagę na art. 28 DSA, który nakazuje dostawcom platform internetowych dostępnych dla małoletnich wprowadzenie odpowiednich i proporcjonalnych środków, aby zapewnić wysoki poziom prywatności, bezpieczeństwa i ochrony małoletnich w ramach świadczonych przez siebie usług. Wspomniani dostawcy platform internetowych nie mogą prezentować w swoim interfejsie reklam opartych na profilowaniu wiedząc z wystarczającą pewnością, że ich odbiorcą jest małoletni użytkownik usług. Wypełnianie przez dostawców platform dostępnych dla małoletnich obowiązków określonych w art. 28 DSA nie zobowiązuje ich do przetwarzania dodatkowych danych osobowych w celu oceny wieku użytkownika.

Sprawa platformy Kick.com była przedmiotem obrad Europejskiej Rady ds. usług cyfrowych we wrześniu 2025 r. w kontekście obowiązku wyznaczenia przedstawiciela prawnego w UE, wynikającego z art. 13 DSA. Platforma ostatecznie wyznaczyła przedstawiciela na Malcie, co oznacza, że właściwym Koordynatorem ds. cyfrowych jest Malta Communications Authority (MCA). Po pełnym wdrożeniu przepisów DSA w Polsce skargi dotyczące działalności Kick.com będą przekazywane przez polskiego Koordynatora, czyli Prezesa UKE do rozpatrzenia Koordynatorowi z Malty.

Z wyrazami szacunku

Michał Gramatyka
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa