Warszawa, dnia 15 grudnia 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

BM-WOP.072.158.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z dnia 24 listopada 2017 r. Posła na Sejm RP Pana Grzegorza Furgo w sprawie *metod gwarantujących bezpieczeństwo w Internecie osób zagrożonych samobójstwem w wyniku ewolucji procesów społecznych i rozwoju narzędzi infotechnologicznych* (interpelacja nr 17071)

Szanowny Panie Marszałku,

przede wszystkim należy podkreślić, że to, co jest nielegalne poza Internetem, jest również nielegalne w Internecie - w tym również nakłanianie do samobójstwa. Zgodnie z przepisami Kodeksu karnego[1] *kto namową lub przez udzielenie pomocy doprowadza człowieka do targnięcia się na własne życie, podlega karze pozbawienia wolności od 3 miesięcy do lat 5*. W przypadku identyfikacji takich treści w Internecie należy je niezwłocznie zgłosić na Policję lub do Prokuratury oraz podmiotu na którego serwerze taka treść/strona została zamieszczona.

Inną kwestią jest odpowiedzialność podmiotów świadczących usługi hostingu (tzw. pośredników internetowych) za działania uniemożliwiające dostęp do danych o bezprawnym charakterze w Internecie oraz szybkość działania w przypadku blokowania dostępu do tego typu treści. W obecnym porządku prawnym, zgodnie z ustawą *o świadczeniu usług drogą elektroniczną*[2], pośrednicy internetowi nie ponoszą odpowiedzialności za dane umieszczane za ich pośrednictwem w Intrenecie, pod warunkiem, że nie posiadają wiedzy o ich nielegalnym charakterze. Pośrednik internetowy po otrzymaniu takiego zawiadomienia (od użytkownika) i jego sprawdzeniu, powinien tego rodzaju treści zablokować. W przypadku zaś otrzymania zawiadomienia urzędowego o bezprawnym charakterze treści, ich zablokowanie powinno nastąpić niezwłocznie.

W przypadku blokowania bezprawnych treści, w tym w szczególności tych zagrażających życiu i zdrowiu osób małoletnich, szybkość działania ma ogromne znaczenie. Dlatego kwestie

[1] Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 2017 r. poz. 2204)
[2] art. 14 ustawa z dnia 18 lipca 2002 r. (t.j.: Dz. U. z 2017 r. poz. 1219)

zarówno odpowiedzialności pośredników internetowych, jak i czasu działania wymagają doprecyzowania w obowiązujących przepisach. Ministerstwo Cyfryzacji rozpoczęło prace nad ujednoliceniem procedury zgłaszania i uniemożliwiania dostępu do danych o bezprawnym charakterze, aby zwiększyć skuteczność wykrywania i usuwania tego typu treści.

Również na forum europejskim podnoszone są zagadnienia dotyczące zwalczania nielegalnych treści w Intrenecie. Mowa jest m.in. o zwiększeniu odpowiedzialności platform internetowych, w celu opracowania szybkich i niezawodnych procedur pozwalających na usuwanie lub uniemożliwianie dostępu do bezprawnych informacji[3] .

W kwestii nowego zjawiska, jakim są gry i rywalizacje online, które mogą zagrażać życiu i zdrowiu małoletnich, trzeba mieć na uwadze również fakt, że są one zjawiskiem trudnym do wykrycia - tzw. „gracze" komunikują się bowiem przez ogólnie dostępne komunikatory (np. poczta elektroniczna), gdzie wyznaczają sobie kolejne zadania lub rywalizacje do wykonania. Konieczne jest zatem prowadzenie działań profilaktycznych na szeroką skalą przy zaangażowaniu i współdziałaniu różnych organów i podmiotów, jak placówki oświatowe i wychowawcze, służby czy organizacje pozarządowe. Tego typu działania są od wielu lat prowadzone zarówno przez Ministerstwo Cyfryzacji, jak i inne podmioty w tym w szczególności Ministerstwo Edukacji Narodowej.

Odnosząc się szczegółowo do postawionych w interpelacji pytań poniżej przedstawiam odpowiedzi:

Ad. 1 Czy Ministerstwo Cyfryzacji prowadzi badania dotyczące forów dyskusyjnych i gier, które mogą bezpośrednio wpływać na zagrożenie życia użytkowników Internetu?

Ministerstwo Cyfryzacji nie prowadzi własnych badań, które odpowiadałyby na pytanie, czy aktywność na forach dyskusyjnych i udział w grach internetowych mogą bezpośrednio wpływać na zagrożenie życia użytkowników Internetu.

Prowadzone są natomiast różne analizy dotyczące celów i częstotliwości korzystania z Internetu. Jednym z takich badań, które obrazują aktywność i zachowania w Internecie młodzieży oraz ich świadomości na temat zagrożeń tam występujących są badania prowadzone przez NASK Dotychczas zrealizowane były dwa takie badania: w 2014 i 2016 r. Wybrane wyniki zostały zaprezentowane w publikacjach „Nastolatki wobec Internetu" oraz „Nastolatki 3.0".

[3] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Zwalczanie nielegalnych treści w Internecie. W kierunku większej odpowiedzialności platform internetowych. COM 92017) 555 final z 28.09.2017 r.

Ad. 2 Jakimi możliwościami w ograniczaniu dostępu do groźnych treści dysponuje Pani resort?

Jednym z celów realizowanych przez Ministerstwo Cyfryzacji jest zapewnienie obywatelom bezpieczeństwa w cyberprzestrzeni. Do naszych zadań należy m.in. opracowywanie i wdrażanie dokumentów strategicznych oraz aktów prawnych z zakresu cyberbezpieczeństwa. Ministerstwo Cyfryzacji we współpracy z innymi podmiotami istotnymi ze względu na zapewnienie bezpieczeństwa cyberprzestrzeni przygotowało m.in. dwa dokumenty, które mają usprawnić i rozwinąć krajowy system cyberbezpieczeństwa. W dn. 27 kwietnia 2017 r. Rada Ministrów przyjęła uchwałą dokument strategiczny - „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”[4]. Intencją KRPC jest osiągnięcie zdolności do skoordynowanych działań w skali kraju, wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom, zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni oraz zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa. Głównym celem jest zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych.

Do wdrażania Polityki opracowany został „Plan działań”, w ramach których budowane i wdrażane będą różne narzędzia mające zapewnić bezpieczeństwo sieci i systemów informatycznych oraz obywateli. Aktualnie zakończyły się jego uzgodnienia ze wszystkimi interesariuszami i została zainicjowana procedura jego przyjęcia.

Jednym z narzędzi przewidzianych w „Planie działań” jest powołane w 2016 r. w NASK Narodowe Centrum Cyberbezpieczeństwa (NC Cyber). Głównym zadaniem Centrum jest dbałość o bezpieczeństwo cyberprzestrzeni RP m.in. poprzez opracowywanie narodowych planów ochrony. NC Cyber współpracuje w tym zakresie z administracją, biznesem oraz ze środowiskiem naukowym. Centrum funkcjonuje jako ośrodek wczesnego ostrzegania, który działając w systemie 24/7/365 monitoruje i zarządza trybem informowania o zagrożeniach sieciowych. Komunikaty o aktualnych niebezpieczeństwach występujących w cyberprzestrzeni, zidentyfikowanych przez NC Cyber zostały w listopadzie br. uruchomione w Regionalnym Systemie Ostrzegania. Centrum zajmuje się również obsługą zgłoszeń szkodliwych i nielegalnych treści (Dyżurnet.pl), w tym w szczególności tych zagrażających młodym użytkownikom Internetu.

W dn. 31 października br. projekt ustawy o krajowym systemie cyberbezpieczeństwa został przekazany do uzgodnień międzyresortowych i konsultacji społecznych. Projekt ustawy (wraz z Oceną Skutków Regulacji i uzasadnieniem) został udostępniony na stronie podmiotowej

[4] Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022

Biuletynu Informacji Publicznej Ministerstwa Cyfryzacji (w zakładce „Prawo i prace legislacyjne Ministerstwa Cyfryzacji ”) oraz na stronie Rządowego Procesu Legislacyjnego[5].

Ad. 3 Czy prowadzone są działania polegające na profilaktyce uświadamiania zwłaszcza młodych ludzi, z zagrożeń, które niesie korzystanie z Internetu?

Zarówno resort cyfryzacji, jak i nadzorowane przez Ministerstwo organy i jednostki, jak Urząd Komunikacji Elektronicznej oraz NASK, prowadzą różnego rodzaju działania mające na celu ochronę dzieci i młodzieży przed nieodpowiednymi treściami w Internecie. Działania te mają charakter w szczególności edukacyjny i skupiają się na obszarze bezpiecznego korzystania z Internetu oraz podnoszenia świadomości o zagrożeniach występujących w sieci. Dotychczasowe działania inicjowane przez Ministerstwo realizowane były głównie poprzez konkursy dla organizacji pozarządowych na realizację zadań publicznych. Ich celem było podnoszenie wiedzy i umiejętności w zakresie bezpiecznego korzystania z Internetu, rozpoznawania zagrożeń oraz przeciwdziałania im. Kierowane były zarówno do dzieci, młodzieży, jak i nauczycieli oraz rodziców. Ministerstwo przyznało dotacje 11. projektom w tym zakresie. W wyniku tych działań wypracowanych zostało wiele materiałów edukacyjnych adresowanych zarówno do wszystkich ww. grup. Przeprowadzone zostały kampanie informacyjne (Internet, media tradycyjne, plakaty, ulotki, konferencje) oraz lokalne szkolenia i warsztaty.

W ramach jednego z takich zadań opracowany został przy współudziale ekspertów z NASK i WSP im. J. Korczaka „*Standard bezpieczeństwa online placówek oświatowych*”, w którym przedstawione zostały procedury interwencji m.in. w przypadkach: cyberprzemocy, groomingu, napotkania nielegalnych treści, sekstingu, czynów zabronionych, nadmiernego korzystania z nowoczesnych technologii oraz reagowania na zagrożenia i incydenty komputerowe. Uwzględniono również zalecenia dotyczące przygotowania bezpiecznej i efektywnej infrastruktury internetowej dla szkoły lub innej placówki oświatowej. W opracowaniu tym zaproponowane zostały zarówno rozwiązania techniczne mające na celu zapewnienie bezpieczeństwa architektury IT placówki, jak i procedury reagowania przez pracowników placówki w przypadku napotkania problemu oraz sposobu właściwego reagowania na dany problem. Wskazane zostały organy, do których należy się zwrócić z problemem, podstawa prawna takiego działania oraz procedura postępowania odnoszącą się do zarówno do sprawcy, jak i ofiary danego zdarzenia. Procedury te zostały opracowane oddzielnie dla rożnych zjawisk i problemów, jak: cyberprzemoc, child grooming (uwodzenie), nielegalne treści (w tym pornograficzne z udziałem osoby nieletniej), seksting oraz incydenty

[5] Wszystkie towarzyszące rządowemu procesowi legislacyjnemu dokumenty (treść uzgodnień międzyresortowych, pisma pomiędzy ministerstwami ws. ustawy, podsumowanie stanowisk w konsultacjach) są dla każdego projektu dostępne na stronie RPL.

komputerowe (technologiczne). Dokument ten został przekazany do Ministerstwa Edukacji Narodowej.

Na szczególną uwagę zasługują działania realizowane przez NASK, który od wielu lat podejmuje szereg inicjatyw związanych z popularyzacją wiedzy o zagrożeniach w Internecie. Za tworzenie oraz realizację działalności szkoleniowej, edukacyjnej oraz popularyzatorskiej Instytutu odpowiada Akademia NASK. Do zadań Akademii NASK należy prowadzenie działań związanych z zastosowaniem technologii informatycznych w społeczeństwie informacyjnym oraz z przeciwdziałaniem wykluczeniu cyfrowemu, w tym szeroko rozumianą tematyką bezpieczeństwa Internetu (w szczególności jego najmłodszych użytkowników). Akademia NASK odpowiada za organizację szkoleń, seminariów i warsztatów związanych z edukacją i popularyzacją idei bezpieczeństwa dzieci i młodzieży oraz prowadzenie różnorodnych akcji i programów edukacyjnych nakierowanych na podnoszenie kompetencji cyfrowych wśród dzieci i młodzieży oraz osób dorosłych. Dla różnych grup, w tym nauczycieli, opiekunów, rodziców, a także przedstawicieli Policji i wymiaru sprawiedliwości organizowane są seminaria, konferencje i spotkania. Ich celem jest podnoszenie poziomu wiedzy m.in. w zakresie wykorzystania nowych mediów w dydaktyce, zagrożeń internetowych i sposobów postępowania w sytuacji problemowej, procedur reagowania i profilaktyki, w tym w szczególności w zakresie zapobiegania i przeciwdziałania cyberprzemocy wśród dzieci i młodzieży, kontaktu ze szkodliwymi treściami, nadużywania Internetu, a także dotyczące problematyki zwalczania przestępstw internetowych popełnianych przeciwko małoletnim.

Ponadto Akademia NASK realizowała inne projekty, które również poruszały jedno z najważniejszych zagrożeń wśród dzieci i młodzieży, jakim jest cyberprzemoc - były to m.in.

- projekt KURSOR (kształcenie umiejętności wykorzystywania nowoczesnych technologii i multimediów w dydaktyce, rozwijanie kompetencji cyfrowych uczniów);
- „Przygody Plika i Foldera w sieci" (przeznaczony dla uczniów szkół podstawowych, którego celem jest zwiększanie świadomości nt. zagrożeń internetowych),
- część edukacyjna pilotażowego projektu OSE – Ogólnopolskiej Sieci Edukacyjnej (celem pilotażu było wdrożenie technicznego modelu dostępu do bezpiecznego szerokopasmowego Internetu w szkołach oraz udostępnienie szkołom multimedialnych aplikacji i serwisów o charakterze edukacyjnym),
- CodeWeek NASK (włączenie instytutu w inicjatywę europejską skierowaną do osób w każdym wieku, zachęcająca do nauki kreatywnego programowania oraz rozszerzająca możliwości wzbogacania kompetencji związanych z kodowaniem).

NASK Organizuje również Kongres Młodych Internautów (KOMIN), warsztaty dla młodzieży oraz konkursy tematyczne. Jednocześnie w ramach NASK funkcjonuje wspomniany wcześniej Dyżurnet.pl, który podejmuje działania wobec nielegalnych treści zgłoszonych przez

użytkowników Internetu lub instytucje. NASK jest także koordynatorem Polskiego Centrum Programu Safer Internet, który realizuje z partnerami kompleksowy program Komisji Europejskiej „Safer Internet". W latach 2016 – 2017 w ramach projektu zorganizowanych zostało wiele wydarzeń edukacyjnych i informacyjnych, w tym kampanię społeczną „Możesz pomóc - reaguj, zgłoś!" prowadzoną przez Dyżurnet.pl – ma ona na celu zwrócenie uwagi na problem skutków, jakie dla ofiar niosą umieszczone w Internecie materiały przedstawiające seksualne wykorzystywanie dzieci. Na stałe do kalendarza wydarzeń z obszaru bezpiecznego Internetu wpisał się Dzień Bezpiecznego Internetu inicjowany przez Safer Internet, obchodzony w szeregu placówek oświatowych i kulturalnych oraz Międzynarodowa Konferencja „Bezpieczeństwo Dzieci i Młodzieży w Internecie". W dniach 19-20 września 2017 r. konferencja ta odbyła się już po raz jedenasty.

Prowadzonych jest więc wiele projektów zarówno krajowych, jak i międzynarodowych, dedykowanych różnym grupom społecznym, wiekowym oraz zawodowym. Oprócz celowych działań i projektów eksperci NASK są obecni w mediach informując o zagrożeniach oraz zasadach bezpiecznego korzystania z Internetu. Komunikaty medialne w dużej mierze kierowane są do dorosłych użytkowników Internetu, w tym do opiekunów i rodziców.

W 2016 r. NASK zrealizował wspomniane już badanie Nastolatki 3.0, którego celem była diagnoza świadomości zagrożeń związanych z użytkowaniem Internetu przez dzieci i młodzież. Wyniki badania stanowią podstawę do planowania dalszych działań i akcji informacyjno-edukacyjnych.

Również UKE realizuje szereg działań edukacyjnych o nazwie „Mój smartfon, mój mały świat" - w formie warsztatów i spotkań bezpośrednio wśród najmłodszych użytkowników Internetu edukuje o bezpiecznych zasadach korzystania z nowych technologii.

Należy podkreślić, że jednym z kierunków wspomnianych Krajowych Ram Polityki Cyberbezpieczeństwa na lata 2017-2022 jest działanie 7.5. *Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli*. Zakłada ono edukacji w zakresie cyberbezpieczeństwa, którą należy rozpoczynać już na etapie kształcenia wczesnoszkolnego. Uwzględniając tematykę bezpiecznego korzystania z cyberprzestrzeni planowane jest opracowanie i wdrożenie zmian do podstaw programowych nauczania. Zakłada się także opracowanie i uruchomienie kursów doszkalających dla nauczycieli informatyki oraz wdrożenie adekwatnych zmian w kształceniu podyplomowym nauczycieli. Równolegle, we współpracy z organizacjami pozarządowymi oraz ośrodkami akademickimi, administracja publiczna podejmie systemowe działania uwrażliwiające społeczeństwo na zagrożenia płynące z w cyberprzestrzeni, a także działania edukacyjne w zakresie praw i wolności w środowisku cyfrowym. Uruchomione zostaną m.in. kampanie społeczne, skierowane do różnych grup docelowych (między innymi dzieci, rodziców i seniorów). Działania te są w trakcie realizacji.

W Ministerstwie Cyfryzacji trwają również prace nad kampaniami edukacyjno-informacyjnymi realizowanymi w ramach działania 3.4 Programu Operacyjnego Polska Cyfrowa (PO PC). Celem kampanii będzie przede wszystkim wskazywanie korzyści korzystania z Internetu oraz promowanie usług administracji publicznej dostępnych w sieci. Podniesione zostaną również kwestie bezpieczeństwa - w ramach planowanych do realizacji od 2018 r. kampanii edukacyjno-informacyjnych nt. technologii cyfrowych przewidziano komponent poświęcony bezpieczeństwu w sieci osób młodych. Będzie to ogólnopolska kampania, której celami będą m.in.:

1. wzrost świadomości zagrożeń związanych z korzystaniem z Internetu.
2. wzrost świadomości dotyczącej zagrożeń wobec dzieci związanych z ich aktywnością w Internecie (cyberprzemoc, sexting, szkodliwe treści).

Jedną z grup, do których będzie kierowana kampania stanowić będą opiekunowie dzieci. Jest to szczególnie istotna grupa z kilku powodów – po pierwsze ze względu na największy wpływ na dzieci, po drugie ze względu na możliwość kontrolowania działań dzieci w Internecie. Grupę tę wybrano ze względu na jej zdiagnozowany niski poziom wiedzy i aktywności w tym zakresie.

Kampania obejmie:

1. realizację sprofilowanej tematycznie kampanii edukacyjno-informacyjnej.
2. publikacje w prasie.
3. publikacje na portalach internetowych oraz działania w mediach społecznościowych.
4. przygotowanie aplikacji mobilnej dotyczącej bezpieczeństwa w sieci.
5. wątki w audycjach i / lub serialach telewizyjnych.

Kampania będzie realizowana w okresie od 2018 do 2020 r.

Z wyrazami szacunku,

Anna Streżyńska
Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów