Warszawa, dnia 14 listopada 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

Anna Streżyńska

BM-WOP.072.146.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. pisma z dnia 25 października 2017 r. Posła na Sejm RP Pana Arkadiusza Marchewki w sprawie *przeciwdziałania cyberprzemocy* (interpelacja nr 16572)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad. 1 W jaki sposób Ministerstwo Cyfryzacji, Ministerstwo Edukacji Narodowej oraz Ministerstwo Spraw Wewnętrznych i Administracji nadzorujące działalność Policji zamierzają wypracować spójny plan przeciwdziałania cyberprzemocy?

Jednym z kierunków wspomnianego w interpelacji dokumentu „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”[1] jest działanie 7.5. - *Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli*. Zakłada ono edukację 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).

Ministerstwo Cyfryzacji we współpracy z członkami Rady Ministrów, kierownikami urzędów centralnych, Dyrektorem Rządowego Centrum Bezpieczeństwa w 2017 r. opracowało Plan

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

działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa. W pracach tych uczestniczyli m.in. przedstawiciele Ministerstwa Spraw Wewnętrznych i Administracji oraz Ministerstwa Edukacji Narodowej. Plan zawiera konkretne działania realizowane przez poszczególne podmioty w zakresie zgodnym z ustawowymi kompetencjami tych podmiotów. Działania znajdujące się w kompetencjach Ministerstwa Edukacji Narodowej są w trakcie realizacji. W nowych podstawach programowych zarówno dla szkół podstawowych[2], jak i ponadpodstawowych[3] uwzględniono kwestie związane z wykorzystywaniem nowych technologii w procesie nauczania, edukacją o bezpieczeństwie w cyberprzestrzeni i krytycznym odbieraniem treści. Zaplanowane zostały również prace mające na celu podnoszenie kompetencji nauczycieli i wychowawców w tym obszarze. Ponadto MEN przygotowało kompendium wiedzy oraz zbiór rekomendacji dotyczących działań profilaktycznych związanych z ryzykiem wystąpienia zagrożeń bezpieczeństwa - w tym w cyberprzestrzeni - w szkole lub placówce wraz ze wskazaniem obowiązujących przepisów i odpowiedzialności pn. „Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów”. Rekomendacje te uwzględniają m.in. problematykę cyberprzemocy oraz procedurę reagowania w przypadku wystąpienia takiego zjawiska. Opracowanie to było konsultowane m.in. z Ministerstwem Cyfryzacji.

Plan działań do Krajowych Ram Polityki Cyberbezpieczeństwa uwzględnia szereg różnych działań informacyjno-edukacyjnych mających na celu podnoszenie świadomości o zagrożeniach występujących w cyberprzestrzeni oraz zasadach bezpiecznego korzystania z Internetu - będą one sukcesywnie realizowane na przestrzeni kolejnych lat. Sporządzony plan jest obecnie w uzgodnieniach z zaangażowanymi w jego tworzenie i realizację podmiotami.

Ad. 2 W jaki sposób skutecznie monitorowane będzie to zjawisko?

Ministerstwo Cyfryzacji monitoruje zjawiska, które mogą oddziaływać na poprawne funkcjonowanie Internetu. Do analizy zjawisk zagrożeń w cyberprzestrzeni, w tym szczególnie groźnych dla dzieci i młodzieży wykorzystywane są różne badania, w szczególności te prowadzone przez NASK. Dotychczas przeprowadzone były dwa badania[4] aktywności dzieci w Internecie (dotyczące również zjawiska cyberprzemocy), których celem była diagnoza świadomości zagrożeń związanych z użytkowaniem Internetu przez dzieci i

[2] Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. 2017 poz. 356)

[3] Projekt rozporządzenia Ministra Edukacji Narodowej w sprawie podstawy programowej kształcenia ogólnego dla czteroletniego liceum ogólnokształcącego, pięcioletniego technikum oraz branżowej szkoły II stopnia

[4] w 2014 i 2016 r.

młodzież. Wybrane wyniki zostały zaprezentowane w publikacjach „Nastolatki wobec Internetu" , „Nastolatki 3.0". oraz „Raport z badania Nastolatki 3.0". Wyniki tych badań stanowią podstawę do planowania dalszych działań oraz akcji informacyjno-edukacyjnych. Badania te będą kontynuowane.

Ad. 3 Czy obecnie podejmowane są działania w skali kraju w celu eliminowania zagrożeń zarówno w zakresie cyberprzemocy, jak i inspirowania do działań niebezpiecznych?

W 2017 r. Ministerstwo Cyfryzacji prowadziło szereg prac o charakterze strategicznym w obszarze cyberbezpieczeństwa. Ich celem była zarówno organizacja krajowego systemu cyberbezpieczeństwa (w dn. 31 października br. został udostępniony do konsultacji projekt ustawy o krajowym systemie cyberbezpieczeństwa), jak również wspominanie już planowanie określonych zadań w skali kraju służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa.

Niezależnie od powyższego obecnie trwają przygotowania do realizacji kampanii edukacyjno-informacyjnych w ramach działania 3.4 Programu Operacyjnego Polska Cyfrowa (POPC). Celem kampanii będzie zwiększenie świadomości Polaków w zakresie wykorzystania technologii informacyjno-komunikacyjnych, w tym wskazywanie zalet w korzystaniu z Internetu, promowanie usług e-administracji publicznej oraz wzrost świadomości, kompetencji i dostępu do wiedzy w zakresie programowania. Ważnym aspektem kampanii będą działania z zakresu edukacji bezpiecznego korzystania z Internetu, możliwych zagrożeń i umiejętności dokonywania racjonalnej ich oceny, a także radzenia sobie z nimi. Podniesione zostaną również kwestie wagi ochrony danych osobowych oraz aspekty dotyczące zagrożeń wobec dzieci związanych z ich aktywnością w Internecie i co za tym idzie – sposobów zabezpieczania ich przed tymi zagrożeniami.

Ponadto na bieżąco realizowane są działania edukacyjne przez podmioty nadzorowane przez Ministerstwo, jak Urząd Komunikacji Elektronicznej oraz wspomniany już NASK. UKE prowadzi projekt edukacyjny 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. Natomiast NASK na bieżąco prowadzi szereg działań związanych z popularyzacją wiedzy o zagrożeniach w Internecie, w tym mających na celu przeciwdziałanie cyberprzemocy. W ramach NASK funkcjonuje Dyżurnet.pl, który podejmuj 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".

Jednocześnie, należy zauważyć, że wyniku przeprowadzonej w 2017 r. bezpośrednio w Ministerstwie Cyfryzacji kontroli pn. „*Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży*", w Wystąpieniu pokontrolnym, w Ocenie kontrolowanej działalności, Najwyższa Izba Kontroli wskazała, że „*NIK ocenia pozytywnie realizację, w kontrolowanym okresie, przez Ministerstwo zadań z zakresu zapobiegania i przeciwdziałania cyberprzemocy wśród dzieci i młodzieży, pomimo stwierdzonych nieprawidłowości w organizacji otwartych konkursów na projekty służące realizacji zadań publicznych w latach 2013-2015. Ministerstwo realizując działania z zakresu bezpieczeństwa cyberprzestrzeni, bazowało między innymi na ogólnodostępnych wynikach badań i opracowań, dotyczących problemów i zagrożeń związanych z cyberprzemocą wśród dzieci i młodzieży zrealizowanych przez Naukową i Akademicką Sieć Komputerową i Fundację Dzieci Niczyje. (…)"*

Z wyrazami szacunku,

Anna Streżyńska
Minister Cyfryzacji
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów