

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ KOMISJI DO SPRAW DZIECI I MŁODZIEŻY (NR 39)

z dnia 24 września 2025 r.

Pełny zapis przebiegu posiedzenia Komisji do Spraw Dzieci i Młodzieży (nr 39)

24 września 2025 r.

Komisja do Spraw Dzieci i Młodzieży, obradująca pod przewodnictwem poseł **Moniki Rosy (KO)**, przewodniczącej Komisji, zrealizowała następujący porządek dzienny:

- **informacja na temat sytuacji dzieci i młodzieży w cyberkonfliktach – odporność placówek oświatowych, organizacji społecznych zajmujących się dziećmi i młodzieżą: ochrona danych osobowych, liczba i rodzaje cyberataków, inne specyficzne wyzwania.**

W posiedzeniu udział wzięli: **Katarzyna Lubnauer** sekretarz stanu w Ministerstwie Edukacji Narodowej wraz ze współpracownikami, **Renata Leoniak** zastępca dyrektora Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji wraz ze współpracownikami, **Monika Pieniek** zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji, insp. **Bartosz Furgała** zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości, **Mirosław Wróblewski** prezes Urzędu Ochrony Danych Osobowych wraz ze współpracownikami, **Katarzyna Hernandez** dyrektor Zespołu Edukacji Cyfrowej i Bezpieczeństwa w Sieci Biura Rzecznika Praw Dziecka, **Andrzej Ross** naczelnik Wydziału do spraw Twórców Treści Internetowych w Departamencie Multimediiów Krajowej Rady Radiofonii i Telewizji wraz ze współpracownikami, **Katarzyna Szymielewicz** prezes Fundacji Panoptykon, **Patryk Chmielecki** i **Aleksandra Więckowska** realizatorzy projektu Future 20, **Nikita Pavlenco**, **Wiktor Pawlikowski** i **Julia Wasilewska** członkowie Rady Młodzieżowej przy Parlamentarnym Zespole do spraw Młodzieży oraz dr **Anna Krawczak** stały doradca Komisji.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Magdalena Kowalska** i **Grażyna Kućmierowska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodnicząca poseł Monika Rosa (KO):

Dzień dobry. Szanowni państwo, wybiła godzina 16.00, więc otwieram posiedzenie Komisji do Spraw Dzieci i Młodzieży.

Witam wszystkich państwa posłów i posłanki oraz zaproszonych gości. Witam sekretarz stanu w Ministerstwie Edukacji Narodowej, panią Katarzynę Lubnauer, wraz ze współpracowniczkami. W imieniu Ministerstwa Cyfryzacji informację przedstawi nam dzisiaj pani Monika Pieniek, zastępca dyrektora Departamentu Cyberbezpieczeństwa. Ze strony Ministerstwa Spraw Wewnętrznych i Administracji są z nami zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości, pan Bartosz Furgała, zastępca dyrektora Departamentu Porządku Publicznego w MSWiA, pani Renata Leoniak, oraz główny specjalista w tymże departamencie, pani Monika Zalewska. Witam przedstawicielkę Biura Rzecznika Praw Dziecka, panią Katarzynę Hernandez. Bardzo serdecznie witam prezesa Urzędu Ochrony Danych Osobowych, pana Mirosława Wróblewskiego. Bardzo dziękuję za pana dzisiejszą obecność wraz ze współpracownikami. Witam również przedstawicieli Krajowej Rady Radiofonii i Telewizji, pana Andrzeja Rossa i pana Artura Kołędę, a także wszystkich zaproszonych gości.

Szanowni państwo, temat dzisiejszego posiedzenia obejmuje rozpatrzenie informacji na temat sytuacji dzieci i młodzieży w cyberkonfliktach, odporności placówek oświatowych i organizacji społecznych zajmujących się dziećmi i młodzieżą, ochrony danych osobowych, liczby i rodzajów cyberataków oraz innych specyficznych wyzwań. Pewnie wszyscy rozumiemy, jak bardzo ważny i trudny jest to temat, nie tylko w Polsce, ale w Unii Europejskiej i na całym świecie. Wiemy doskonale, jak cyberkonflikty wpływają na dzieci.

W 2022 r. ukazał się bardzo ważny raport Funduszu Narodów Zjednoczonych na rzecz Dzieci (UNICEF) „Protecting Children in Cyberconflicts”, który w Polsce nie odbił się zbyt szerokim echem, natomiast pokazał bardzo jasno, jak nowe narzędzia umożliwiają ukryte i długofalowe ataki na dzieci i na infrastrukturę cywilną, wykorzystywanie danych osobowych dzieci

i młodzieży oraz ataki na placówki edukacyjne, które później wpływają na bezpieczeństwo całego społeczeństwa. Raport pokazał, jak wielka jest różnorodność tych ataków, jak różne formy one przyjmują i jak wiele rodzajów ryzyka istnieje w kwestiach manipulacji dziećmi, rekrutacji ich do grup skrajnych i ekstremalnych, wykradania danych osobowych nie tylko dzieci i młodzieży, ale także nauczycieli albo rodziców, ataków na infrastrukturę szkolną, ale także na infrastrukturę krytyczną.

Generalnie stoimy teraz przed ogromnym wyzwaniem. Są także badania, które pokazują, że również dzieci stoją za tymi atakami. Dane brytyjskiego komisarza do spraw informacji wskazują, że sprawcami 57% incydentów w szkołach nie byli zewnętrznymi cyberprzestępcy, lecz właśnie uczniowie, a 30% tych incydentów było spowodowanych tym, że po prostu zgadywali oni hasła, które funkcjonowały w placówkach edukacyjnych. Wiemy doskonale, że od zabawy do poważnych ataków jest naprawdę dość blisko.

Doskonale wiemy też, jak bardzo nieprawdziwe jest to, co mówią przedstawiciele platform społecznościowych, że chronią dzieci, które dopiero od 13. roku życia mają do nich dostęp. Grupy ekstremistyczne, bojówki i skrajne organizacje na platformach tego typu i na platforma gamingowych mogą wpływać na dzieci oraz młodzież, manipulować nimi, rekrutować je do swoich działań, budować ich zaufanie, a później wykorzystywać właśnie jako narzędzia w cyberkonfliktach. Dlatego tak ważne jest to posiedzenie i dlatego dziękuję za państwa obecność.

Jako pierwszą poproszę o zabranie głosu panią ministram Katarzynę Lubnauer.

Sekretarz stanu w Ministerstwie Edukacji Narodowej Katarzyna Lubnauer:

Przede wszystkim chciałabym powiedzieć, że mają państwo większość materiału, bo wszyscy posłowie otrzymali informację MEN.

Musimy natomiast zdać sobie sprawę z tego, że kwestie cyberbezpieczeństwa, bezpieczeństwa dzieci w sieci, ale również tego wszystkiego, co wiąże się z profilaktyką i edukacją, a co pozwala nam nauczyć dzieci, jak być bezpiecznymi, to jest jedno z największych wyzwań dla MEN. Działania na tym polu są wielorakie.

Przede wszystkim w ostatnich latach pojawiły się one w kierunkach polityki oświatowej. W 2024 r. znalazły się tam zagadnienia związane ze źródłami informacji w przestrzeni, ale również z dobrostanem psychicznym, empatią i edukacją włączającą. Również w 2025 r. pojawiła się profilaktyka przemocy rówieśniczej, higiena cyfrowa i krytyczna analiza informacji. Jak widać, to są rzeczy dla nas priorytetowe, ponieważ kierunki polityki oświatowej wskazują dość jednoznacznie wszystkim placówkom doskonalenia nauczycieli, w jakim kierunku iść.

Kolejną rzeczą jest to, że ministerstwo przygotowało całościowy materiał, jakim jest „Polityka cyfrowej transformacji edukacji”. Materiał jest uchwałą rządu. Poza faktem, w jaki sposób ma się zmieniać edukacja, jeśli chodzi o kwestię cyfryzacji, uchwała wskazuje również, w jaki sposób zabezpiecza się i dba o to wszystko, co jest związane z higieną cyfrową i z kwestią bezpieczeństwa.

Następnym elementem, który jest dla nas bardzo ważny, są kwestie związane z programami wychowawczo-profilaktycznymi w szkołach. Materiały uchwalane przez radę rodziców i radę pedagogiczną obejmują również zagrożenia związane z cyberbezpieczeństwem. Szkoły wspiera w tym Ośrodek Rozwoju Edukacji (ORE), który tworzy bazę dobrych praktyk, co pomaga szkołom w przygotowywaniu takich programów.

Kolejnym elementem są nowe przedmioty oraz podstawa programowa. Pamiętajmy, że w tym roku w podstawie programowej pojawiają się dwa nowe przedmioty. Oba uwzględniają zagadnienia związane z cyberbezpieczeństwem. Elementy dotyczące zagrożeń związanych z cyberprzestrzenią są bardzo widoczne w edukacji zdrowotnej, zarówno jeśli chodzi o formy cyberprzemocy, jak również o kwestię uzależnień. To wszystko jest bardzo ważnym elementem edukacji zdrowotnej. Zdrowie psychiczne jest tam jednym z ważniejszych komponentów, co wskazuje na to, w jaki sposób uczulamy dzieci i młodzież na te zagrożenia. Kolejnym przedmiotem jest edukacja obywatelska, gdzie na przykład jest mowa o dezinformacji i o rzeczach, które wiążą się z tym, co też jest formą cyberprzemocy.

Zauważmy jednak, że to jest dopiero początek zmian, ponieważ przypomnę, że w 2026 r. do szkół wchodzi reforma. Mówię o programie „Reforma26. Kompas jutra”. Na zajęciach z języka polskiego pojawia się na przykład moduł edukacji medialnej, który również obejmuje te zagadnienia. Oczywiście poza informatyką, na której są poruszane zagadnienia związane

z cyberbezpieczeństwem, również na języku polskim będziemy mieli moduł medialny, który na przykład mówi o dezinformacji i o rzetelnych lub nierzetelnych źródłach wiedzy.

Kolejną kwestią jest pomoc psychologiczno-pedagogiczna. Pamiętajmy, że wchodzą coraz wyższe standardy dotyczące pomocy psychologiczno-pedagogicznej. Teraz głównie zajmujemy się tym, żeby likwidować białe plamy. Muszę przyznać, że jak weszliśmy do ministerstwa, to okazało się, że mamy jednak bardzo dużo gmin, w których nie ma realnej pomocy psychologicznej. W tej chwili staramy się, żeby tych obszarów, które są pozbawione owego wsparcia, było jak najmniej.

Następnie mamy takie inicjatywy MEN, jak „Szkoła dostępna dla wszystkich”, szkolenia dla nauczycieli i specjalistów, „Wolontariat na rzecz wsparcia rówieśniczego w ochronie zdrowia psychicznego dzieci i uczniów” czy rozwój kompetencji cyfrowych nauczycieli. Chciałabym powiedzieć, że ruszają szkolenia dla 88 tys. nauczycieli, które dotyczą zarówno wykorzystania sztucznej inteligencji, jak również umiejętności cyfrowych. Szkolenia są też organizowane dla koordynatorów. Zresztą w ciągu ostatnich lat tych szkoleń naprawdę było bardzo wiele, dlatego że wiemy, jak ważne jest to, żeby również nauczyciele zdawali sobie sprawę z zagrożeń, które cyhają w internecie.

Kolejna jest kwestia konkursu „Zobacz emocje”. Powstają projekty psychoedukacyjne.

Kuratoria bardzo silnie włączają się w te działania, jak również w to, żeby chociażby zabezpieczać dane. Pamiętajmy o tym, że edukacja to jest też ogromny obszar danych, na przykład związanych z egzaminami czy z informacjami o uczniach. W związku z tym naszym zadaniem, jeśli chodzi o cyberbezpieczeństwo, jest również zabezpieczanie danych uczniów. To też jest ważny obszar.

Organizujemy też takie wydarzenia tematyczne, jak dzień bezpiecznego internetu. W konkursie, który współorganizujemy razem z Urzędem Ochrony Danych Osobowych (UODO), uczulamy uczniów na kwestię ochrony swoich danych i wizerunku. Przykładem jest program „Twoje dane – Twoja sprawa”. W taki sposób dzieci uczą się, że wszystko, co wrzucą do internetu, już nigdzie nie ginie i zawsze może być obrócone przeciwko nim.

W tym bardzo szerokim obszarze MEN podejmuje wiele działań, które mają charakter profilaktyczny i wychowawczy czy też są związane ze zdrowiem psychicznym. Włączamy się także w te obszary, które są związane bezpośrednio z cyfryzacją, czyli tym wszystkim, co zadecyduje o cyfrowej transformacji edukacji. Z jednej strony ma się to odbyć z wykorzystaniem wszystkich elementów, które są nie tylko bezpieczne, ale i sprzyjające rozwojowi dziecka, a jednocześnie chodzi o takie działania, które powodują, że wszystko to ma się dzieć w bezpiecznej atmosferze.

Muszę powiedzieć, że w tej chwili odbywa się wiele dyskusji o zakazach korzystania w szkole ze sprzętów. W ustawie o rzeczniku praw ucznia, która – jak myślę – w najbliższym czasie trafi do Sejmu, wprowadzamy zasadę, że szkoły mogą wzmocnić swoją rolę decyzyjną, wprowadzając całkowity zakaz wykorzystywania smartfonów, bo też zależy nam na tym, żeby z punktu widzenia uczniów szkoła była miejscem jak najbardziej bezpiecznym, zarówno jeśli chodzi o uzależnienia, jak i o to wszystko, co jest elementem cyberprzemocy. Myślę, że resztę mają państwo w materiale.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję, pani ministro.

Poproszę teraz panią Monikę Pieniek z MC o równie syntetyczną wypowiedź, bo i tak mamy materiały od państwa.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Monika Pieniek:

Dziękuję bardzo.

Szanowna pani przewodnicząca, szanowni państwo, chciałabym się odnieść do ataków na infrastrukturę placówek oświatowych. W tym zakresie przedstawię państwu aktualne dane. Nie muszę o tym wspominać, ale powinnam, że Polska jest obecnie jednym z najczęściej atakowanych w cyberprzestrzeni państw na świecie. W ubiegłym roku wszystkie trzy zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) obsłużyły ponad 110 tys. ataków. Przypomnę tylko, że takie zespoły działają w trzech instytucjach. Jedną jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (CSIRT NASK), drugą jest Agencja Bezpieczeństwa Wewnętrznego (CSIRT GOV), a trzecią jest Ministerstwo Obrony Narodowej

(CSIRT MON). W zeszłym roku zatem trzy zespoły CSIRT obsługiwały ponad 110 tys. cyberincydentów, co stanowi wzrost o około 23% w stosunku do roku poprzedniego, natomiast w pierwszej połowie tego roku obsłużono już ponad 100 tys. incydentów. Sądzymy więc, że obecny rok będzie niestety kolejnym rokiem rekordowym w tym zakresie.

Odnosząc się jednak do placówek oświatowo-wychowawczych, muszę zauważyć, że tam również niestety wzrasta liczba cyberataków. Nie jest to jednak aż tak dramatyczny wzrost, ale też tych ataków nie jest tak dużo. Teraz już przedstawię państwu szczegóły, bo chciałabym zaprezentować tutaj statystyki. Otóż na przestrzeni ostatnich lat, od 2022 r. do września br., widać wzrost liczby incydentów również w tych placówkach.

Dla przykładu podam, że sam CSIRT NASK, który jest właściwy do zgłaszania incydentów dla tego rodzaju placówek, czyli to on je obsługuje, w 2022 r. obsłużył 167 takich incydentów, co stanowi 0,4% w stosunku do wszystkich incydentów, które zostały obsłużone przez trzy zespoły CSIRT w 2022 r. W 2023 r. doszło do 354 cyberincydentów, ale zgodnie z trendem wzrostowym, który w ogóle dotyczył też globalnej skali incydentów, ten odsetek również kształtował się na poziomie 0,4%. Tak jak powiedziałam, w 2024 r. liczba incydentów była rekordowa, a zatem również tutaj był widoczny wzrost. Zgłoszono 733 incydenty w placówkach oświatowych, co stanowiło 0,6% udziału we wszystkich obsłużonych incydentach. Natomiast dokładnie do 22 września br. dla sektora obejmującego placówki oświatowe odnotowano już 895 incydentów, co stanowi niemal 0,9% zgłoszonych i obsłużonych przez NASK incydentów.

Należy jednak podkreślić, że statystyki, o których przed chwilą nadmieniłam, obejmują cały system oświaty i wychowania, tj. przedszkola, szkoły podstawowe i ponadpodstawowe, zespoły szkół, ośrodki wychowawcze i biblioteki, a także uczelnie. Właśnie uczelnie to bardzo ważna sprawa, bo liczby, które przed chwilą państwu przedstawiłam, w jednej trzeciej dotyczyły ataków na uczelnie. Dlaczego tak się dzieje? Otóż naszym zdaniem wynika to z tego, że grupy hakerskie powiązane z wrogimi rządami są zainteresowane przejęciem danych dotyczących nowych technologii, badań i własności intelektualnej, a to jest właściwe akurat dla uczelni.

Zwiększająca się liczba zgłoszeń incydentów w zakresie cyberbezpieczeństwa, a to też jest istotne, świadczy nie tylko o wzmożonych działaniach cyberprzestępców, ale oznacza również wzrost świadomości społecznej na temat konieczności ich zgłaszania do odpowiednich podmiotów, co przynosi wymierne korzyści. Warto podkreślić, że rzeczywista skala cyberataków na omawiane placówki może być jednak większa, gdyż zapewne nie zawsze wszystkie jednostki oświatowe zgłaszają każdy incydent. Wynikać to może zarówno z mniejszej świadomości zagrożeń wśród użytkowników i administratorów, jak również wiązać się z niechęcią do ujawniania zdarzeń, które mogłyby stawiać instytucję w niekorzystnym świetle.

Analizując incydenty według ich rodzajów, należy wskazać, że najczęstszym rodzajem incydentów jest phishing, czyli oszustwa oparte na socjotechnice. Dla przykładu podam, że w 2022 r. w placówkach oświatowych i wychowawczych NASK odnotowała 71 takich incydentów. W 2023 r. było ich 180, w 2024 r. – już 512, natomiast do 22 września br. odnotowano 676 incydentów typu phishing.

Zdarzają się też incydenty z zakresu uruchamiania złośliwego oprogramowania. Szczególnie w 2025 r. odnotowano 102 takie zgłoszenia. Warto właśnie zwrócić uwagę na problem incydentów związanych z uruchomieniem złośliwego oprogramowania, a w szczególności incydentów typu *ransomware*, czyli oprogramowania, które jednocześnie szyfruje dane w celu wymuszenia okupu. Choć te incydenty stanowią mniejszość, to ich liczba również wzrasta z 3 przypadków w 2022 r. do 9 przypadków w 2024 r. Natomiast w 2025 r. do teraz odnotowano 7 takich przypadków. Ataki typu *ransomware* wiążą się ze szczególnym zagrożeniem. Mogą bowiem prowadzić do sparaliżowania funkcjonowania podmiotu, a także do bezpowrotnej utraty danych, jeżeli niezgodnie z dobrymi praktykami nie były robione odmiejszczone kopie bezpieczeństwa.

Zatem, jak państwo usłyszeli, incydentów w globalnej skali nie jest tak dużo, prawda? Oczywiście zdarzają się, ale chciałabym podkreślić niski poziom liczby incydentów w szkołach podstawowych i średnich, na co kluczowy wpływ ma jedność działań rozwijanych przez ministra cyfryzacji.

Wśród nich jest Ogólnopolska Sieć Edukacyjna (OSE). Operatorem OSE, czyli dostawcą szybkiego internetu do szkół, jest NASK, a więc instytucja nadzorowana przez ministra cyfryzacji. Usługa „Bezpieczny internet”, która jest świadczona w ramach sieci OSE, ma na celu zapewnienie m.in. ochrony szerokopasmowego dostępu do internetu przed szkodliwym oprogramowaniem.

Monitoruje ona również zagrożenia i bezpieczeństwo sieciowe oraz przeciwdziałania dostępowi do treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju dzieci i młodzieży. Usługa ta jest włączana domyślnie wraz z rozpoczęciem świadczenia OSE w szkole. „Bezpieczny internet” realizuje funkcje ochronne w zakresie blokowania niepożądanego komunikacji sieciowej, a także pozwala na zabezpieczenie sieci szkolnej w podstawowym zakresie. Jednakże jest też możliwość rozszerzenia tej usługi o dodatkową ochronę, w tym na przykład o ochronę tablic interaktywnych, monitorów multimedialnych, gogli VR czy telewizorów smart, a także urządzeń mobilnych. Jest więc i taka możliwość.

Może dodałabym jeszcze, że w ramach nowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa (KSC) będziemy również wzmacniać cyberbezpieczeństwo w szkołach podstawowych i ponadpodstawowych. Jednostki te po prostu będą musiały wdrożyć dodatkowe zabezpieczenia, które zostały określone w załączniku nr 4 do tejże ustawy. Wymogi mają charakter listy kontrolnej minimalnych wymagań dla tego rodzaju systemów, jak inwentaryzacja zasobów informatycznych, weryfikacja uprawnień personelu, stosowanie oprogramowania antywirusowego czy przestrzeganie zasad higieny. Włączenie tych zadań do ustawy o KSC gwarantuje też większą ochronę i aktywność ze strony zespołu CSIRT NASK, o którym tutaj mówiłam.

Chciałabym jeszcze wspomnieć o jednym narzędziu, o którym jest mowa w materiale, jaki został przekazany Komisji. W zakresie cyberbezpieczeństwa placówki oświatowe są wspierane również poprzez system Artemis. To specjalny system, który jest w dyspozycji zespołu CSIRT NASK. Służy on do skanowania serwisów internetowych w celu znalezienia podatności i przekazania o nich informacji do odpowiednich osób, które zarządzają daną stroną. W 2024 r. NASK przeskanowała ogółem 249 806 domen i adresów IP oraz 795 547 subdomen. Natomiast jeżeli chodzi o strony szkół podstawowych, ponadpodstawowych i policealnych, domy młodzieży i domy kultury, przedszkola oraz poradnie psychologiczne, to również one znalazły się na tej liście, z której dane przed chwilą wymieniałam. W kategorii tych podmiotów przeskanowano 67 509 domen oraz adresów IP i ponad 281 tys. subdomen. Co to oznacza? Jeżeli jakkolwiek podatność została znaleziona podczas skanowania, to NASK zawiadamiała administratora takiej strony o danej podatności z prośbą o jej usunięcie. To tyle. Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Teraz proszę upoważnione osoby ze strony MSWiA. Bardzo proszę.

Zastępca dyrektora Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji Renata Leoniak:

Dziękuję bardzo. Renata Leoniak, zastępca dyrektora Departamentu Porządku Publicznego. Przygotowaliśmy krótką prezentację, którą przedstawilibyśmy tutaj wspólnie z panem komendantem.

Na początku chcieliśmy krótko powiedzieć o najczęstszych incydentach, które zdarzają się w szkołach, przedszkolach i organizacjach pozarządowych. Jak wcześniej mówiła już o tym pani dyrektor, jednymi z najczęstszych są ataki *ransomware*.

Kolejne są kampanie phishingowe. Ich celem jest kradzież danych osobowych dzieci i pracowników bądź uzyskanie danych wrażliwych lub umożliwiających dostęp do bankowości elektronicznej.

Identyfikujemy takie przypadki, kiedy dziecko jest wykorzystywane jako element kampanii celowanej w rodziców. Oszuści nawiązywali kontakty z rodzicami za pomocą esemesów, informując ich o rzekomej utracie telefonu przez dziecko i o konieczności przelania środków finansowych na zakup nowego urządzenia.

Następnym przypadkiem są ataki DDoS, które paraliżują funkcjonowanie dzienników elektronicznych, serwerów e-learningowych i systemów rekrutacyjnych. Zauważalny był wzrost tych ataków, gdzie atakowano szkoły i placówki społeczne posiadające symbolikę ukraińską czy też fundacje pomagające uchodźcom oraz strony wspierające edukację obywatelską. Ataki te dotyczyły dzienników elektronicznych, na przykład Vulcan czy Librus. Prowadziły one do wycieku danych osobowych i medycznych uczniów.

Ostatnim największym atakiem phishingowym w Polsce był atak dokonany w maju 2020 r., kiedy to przestępcy stworzyli fałszywe strony internetowe importujące portal Librus. Tak wówczas, jak i obecnie celem takich ataków były i są dane do logowania użytkowników.

Chcielibyśmy jeszcze zwrócić uwagę na fałszywe powiadomienia o podłożeniu ładunków wybuchowych. Celem tych ataków w latach 2018–2025 były m.in. właśnie placówki oświatowe. W latach 2019–2023 zauważalny był trend nasilania się powiadomień w okresach egzaminów maturalnych i gimnazjalnych. W 2024 r. odnotowano 117 pojedynczych powiadomień o podłożeniu ładunku wybuchowego oraz 28 powiadomień kaskadowych. Natomiast w roku bieżącym odnotowano 49 powiadomień pojedynczych oraz 24 powiadomienia kaskadowe.

Zwracamy jeszcze uwagę na to, że dzieci i młodzież w cyberprzestrzeni są nie tylko ofiarami, ale także nieświadomymi uczestnikami konfliktów. Do najczęściej identyfikowanych problemów współczesnej młodzieży, które jako resort zauważamy, należą przede wszystkim uzależnienia od internetu, telefonu, mediów społecznościowych i gier komputerowych, a także cyberprzemoc, czyli nękanie i zastraszanie oraz grożenie publikacją wizerunku. W ramach tych cyberataków, które destabilizują środowisko edukacyjne, dochodzi do przerywania zajęć zdalnych czy utraty materiałów edukacyjnych, a także do cyberprzemocy między uczniami w kanałach komunikacyjnych.

Do kolejnych problemów zalicza się dezinformację i manipulację emocjonalną. Dzieci są celem kampanii manipulacyjnych w czasie konfliktów, na przykład poprzez fałszywe wiadomości o zagrożeniach, wyzwania typu *challenge* w mediach społecznościowych czy też złośliwe linki rozsyłane w klasowych czatach.

Należy jeszcze zwrócić uwagę na używanie dzieci jako pewnego rodzaju – w cudzysłowie – przekaźników danych. Konta uczniów są wykorzystywane do rozsyłania zainfekowanych plików lub próśb o dane finansowe.

Z perspektywy MSWiA najistotniejsze zadania w obszarze zwalczania cyberprzestępczości realizuje Centralne Biuro Zwalczania Cyberprzestępczości. Właśnie tutaj chciałabym przekazać głos panu komendantowi, który zaprezentuje najważniejsze informacje o działaniach tego biura. Dziękuję bardzo.

Zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości insp. Bartosz Furgała:

Dziękuję uprzejmie.

Szanowna pani przewodnicząca, szanowni państwo, to, o czym mówiła pani dyrektor, to są oczywiście zagrożenia, które stanowią dla nas bardzo istotny społecznie problem. Natomiast z punktu widzenia Policji część tych zagrożeń stanowią oczywiście czyny zabronione, o czym chciałem pokrótce państwu powiedzieć.

Jak z naszej perspektywy wygląda ta optyka? Jeśli chodzi o Policję, jak państwo doskonale wiedzą, CBZC jest jednostką organizacyjną Policji, która jest wyspecjalizowana w sprawach realizacji zadań dotyczących rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego i teleinformatycznego oraz sieci teleinformatycznej. Zajmujemy się oczywiście również zapobieganiem tego rodzaju przestępstwom oraz wykrywaniem i ściganiem ich sprawców. Na slajdzie widzą państwo obszary naszej działalności. To praca operacyjna, praca śledcza, profilaktyka i coś, co nazwalibyśmy *emergency*, a co będzie miało kluczowy wpływ na temat naszej dzisiejszej dyskusji.

Powiem bardzo ogólnie, jak to wygląda z perspektywy Policji w liczbach. Według naszych danych, pochodzących oczywiście ze zbiorów krajowego systemu informacyjnego Policji (KSIP), jeśli chodzi o osoby małoletnie, to zostały one pokrzywdzone bardzo szeroko rozumianymi przestępstwami z zakresu cyberprzestępczości, które były różne – od hi-tech, przez oszustwa internetowe, po znieważenia w sieci internet. Odnotowano 1451 przestępstw na szkodę 1518 małoletnich. To są dane za okres od stycznia do 21 września br. Mamy oczywiście świadomość, że są to dane dotyczące przestępstw zgłoszonych lub ujawnionych przez Policję. Ich skala na pewno jest większa.

Jeśli chodzi o to, co w ramach tego zakresu realizuje CBZC, to wspomnę, że w tym roku prowadziliśmy 221 postępowań z tej skali, o której państwu powiedziałem. Jak państwo mogą zauważyć w zielonej tabeli, najczęstszymi przestępstwami na szkodę małoletnich są rozpowszechnianie treści pedofilskich i pornograficznych z udziałem małoletnich oraz posiadanie treści pornograficznych z udziałem małoletniego.

Zanim przejdę do działalności profilaktycznej, chciałbym powiedzieć, że ten medal ma także i drugą stronę, bo posiadamy dane, które wskazują na to, jaki jest udział osób nieletnich w skali popełnianych przestępstw i czynów karalnych. Z naszych statystyk wynika, że w 2025 r.,

do chwili obecnej, mieliśmy 242 nieletnich podejrzanych o czyny z zakresu szeroko rozumianej cyberprzestępczości. Z perspektywy CBZC widzimy, że wiek sprawców czynów cyberprzestępczych się obniża. Sprawcami bardzo zaawansowanych ataków *ransomware* czy DDoS są coraz młodsze osoby, w tym małoletni.

Jeśli chodzi o naszą działalność cyberprofilaktyczną, jak o niej mówimy, cała Policja, oczywiście oprócz ścigania i wykrywania przestępstw, prowadzi działalność ukierunkowaną na inicjatywę profilaktyczną. W całej Policji było ponad 26 tys. spotkań, w których uczestniczyło ponad 700 tys. osób, w tym dzieci i młodzież.

Mając natomiast na względzie naszą doniosłą rolę w systemie zapobiegania cyberprzestępczości, jesteśmy w pełni świadomi, że profilaktyka jest jedyną drogą do tego, żeby eliminować cyberprzestępczość ogólnie, a nie tylko zagrożenia dla dzieci i młodzieży, o czym przekonuje się cały świat, który zwraca się w stronę profilaktyki. Wiemy bowiem o tym, że ściganie sprawców tych przestępstw i doprowadzenie ich przed wymiar sprawiedliwości jest bardzo trudne, a czasem wręcz niemożliwe.

Dlatego też rozwijamy sieć swoich cyberprofilaktyków. Każdy z naszych zarządów, a jest ich 18 w kraju, ma jedną taką osobę. W tym momencie jesteśmy jeszcze małą jednostką, bo rozwijamy się dopiero od trzech lat. Mamy więc po jednej dedykowanej osobie na województwo, która nie zajmuje się niczym innym, a wyłącznie prowadzeniem zajęć profilaktycznych z różnymi grupami wiekowymi – z dziećmi i młodzieżą, z seniorami, z osobami czynnymi zawodowo i aktywnymi. W 2024 r. mieliśmy 160 takich spotkań edukacyjnych, w których uczestniczyło 16 tys. dzieci i młodzieży. Proszę zobaczyć na slajdzie, że w roku bieżącym mamy już 621 takich spotkań, w których uczestniczyło 45 tys. dzieci i młodzieży.

Poza tym, jeśli chodzi o profilaktykę, chciałbym dodać, że jesteśmy też członkami europejskiej sieci prewencyjnej, która działa przy Europolu. Jest to International Cyber Offender Prevention Network (InterCOP). W ramach sieci InterCOP realizujemy bardzo ciekawe i fajne inicjatywy.

Jako przykład mogę podać to, co realizowaliśmy już w tym roku, i będziemy jeszcze raz to robić. Chodzi o ataki DDoS. Jeśli młody człowiek chciałby przeprowadzić atak DDoS, który polega na tym, żeby w jednym czasie uderzyć i w bardzo szeroki sposób zainspirować dużą liczbę odsłon na jakiejś stronie internetowej lub skorzystać z jakiejś usługi internetowej, powodując paraliż całego systemu, to musi dowiedzieć się, jak to zrobić. Wpisuje więc w popularnych przeglądarkach zapytanie, jak przeprowadzić atak DDoS. Współpracując z siecią InterCOP, mieliśmy pozycjonowanie, jeśli chodzi o wyniki wyszukiwania, więc na pierwszym miejscu, kiedy młody człowiek odpytywał wyszukiwarkę, otrzymywał odpowiedź, że CBZC ostrzega: „Uważaj, DDoS to przestępstwo. Nie popełniaj go. Stań po dobrej stronie”.

To są takie kampanie, które będą cyklicznie realizowane. Cieszy nas też fajny ich wymiar i bardzo dobry odbiór społeczny. To są tematy, które realizujemy w ramach cyberprofilaktyki. Robimy to w formie warsztatów, spotkań, teatru i bardzo różnych interaktywnych zajęć. To są te tematy, które realizujemy z dziećmi i młodzieżą.

Jeśli chodzi o działalność naszego biura, chciałbym jeszcze powiedzieć o tym, co uważam za szczególnie istotne dla funkcjonowania w obszarze zagrożeń dla dzieci i młodzieży. To jest seksualne wykorzystywanie dzieci w sieci. Nasze biuro od 2022 r. cyklicznie prowadzi akcje ukierunkowane na sprawców seksualnego wykorzystywania osób małoletnich i udostępniania w sieci materiałów przedstawiających takie wykorzystywanie.

Mieliśmy do tej pory sześć akcji, a istniejemy od trzech lat. W ramach tych akcji dokonaliśmy ponad 6 tys. przeszukań, zabezpieczyliśmy ponad 2,4 mln plików z takim contentem, 377 osób usłyszało zarzuty, a 163 osoby decyzją polskich sądów zostały tymczasowo aresztowane.

Nadal będziemy prowadzić tę działalność. Chcemy ją rozwijać. Ostatnia nasza akcja o kryptonomimie „FEVER” obejmowała kilkanaście krajów Unii Europejskiej. Była ona związana z naszą prezydencją w UE. W tym obszarze będziemy kontynuować zwalczanie tego rodzaju zagrożeń.

Ostatnia rzecz, o której chciałbym powiedzieć, to jest coś nietypowego, jeśli chodzi o cyberobszar, bo żadna jednostka na świecie, która się zajmuje cyberprzestępcstwami, nie realizuje tego typu zadań. To coś, co tak naprawdę jest efektem tego, o czym dzisiaj mówimy, czyli zagrożeń dla dzieci i młodzieży, cyberkonfliktów, hejtu w internecie, różnych trudnych sytuacji, znieważnień i gróźb bezprawnych, które często doprowadzają młode osoby do podjęcia bardzo trudnej decyzji, a przynajmniej komunikowania o tym, że chcą odebrać sobie życie.

Jesteśmy tą jednostką, która monitoruje sieć internet oraz współpracuje z kilkoma instytucjami, a może nawet już kilkunastoma, m.in. z Biurem Rzecznika Praw Dziecka, z Fundacją Dajemy Dzieciom Siłę, z platformą 116sos.pl i z Towarzystwem Przyjaciół Dzieci.

Na czym polega ta działalność? Monitorując sieć oraz otrzymując sygnały ze wszystkich infolinii o tym, że ktoś zadeklarował w sieci internet chęć odebrania sobie życia, dokonujemy stosownych ustaleń. To dzieje się 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, więc jesteśmy tutaj cały czas na posterunku. Ustalamy wszystkie możliwe dane dotyczące lokalizacji człowieka i dyslokujemy tam patrol lokalnej jednostki Policji do podjęcia skutecznych działań.

Proszę zobaczyć, szanowni państwo, jak wyglądają statystyki. W 2024 r. jako CBZC mieliśmy prawie 3 tys. zgłoszeń, z czego ponad 1,7 tys. dotyczyło małoletnich, przy czym 842 osoby małoletnie wymagały hospitalizacji, a 887 małoletnich przekazano pod opiekę dorosłych. To jest stan na koniec sierpnia br. Mieliśmy już prawie 1,8 tys. zgłoszeń, z których niemal 1050 dotyczyło małoletnich, przy czym około 600 małoletnich wymagało hospitalizacji, a prawie 500 przekazano pod opiekę osobie uprawnionej. Mamy więc świadomość naszej doniosłej roli w tym systemie. Tu również będziemy kontynuować nasze wysiłki.

Na marginesie chciałbym jeszcze powiedzieć o tym, że bardzo duże nadzieje wiążemy z projektem nowelizacji ustawy o świadczeniu usług drogą elektroniczną, która dotyczy blokowania treści w internecie. Mamy nadzieję, że to też w bardzo dużym stopniu ułatwi nam realizację zadań dotyczących przeciwdziałania tego rodzaju przestępczości. Dziękuję bardzo.

Zastępca dyrektora departamentu MSWiA Renata Leoniak:

Dzięki.

Pani przewodnicząca, jeśli można...

Przewodnicząca poseł Monika Rosa (KO):

Bardzo proszę.

Zastępca dyrektora departamentu MSWiA Renata Leoniak:

Dodałabym coś jeszcze o realizowanym w ministerstwie rządowym programie ograniczania przestępczości i społecznych zachowań „Razem bezpieczniej”. W ramach tego programu na lata 2025–2028 bierzemy pod uwagę wyzwania współczesnego świata i rodzące się zagrożenia, a w szczególności właśnie w odniesieniu do dzieci i młodzieży. Jeden z celów tego programu jest związany z tworzeniem, rozwijaniem i doskonaleniem kompetencji społecznych w zakresie cyberbezpieczeństwa. Działania w tym obszarze odnoszą się głównie do cyberhigieny, czyli takich zagadnień, jak bezpiecznie korzystać z internetu i urządzeń cyfrowych. Są one skierowane do wszystkich grup wiekowych, a dotyczyć będą też edukacji w zakresie identyfikacji i przeciwdziałania dezinformacji w cyberprzestrzeni. Dziękujemy bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Bardzo proszę o zabranie głosu prezesa UODO pana Mirosława Wróblewskiego.

Prezes Urzędu Ochrony Danych Osobowych Mirosław Wróblewski:

Bardzo dziękuję.

Szanowna pani przewodnicząca, szanowna pani minister, szanowni państwo, działania podejmowane przez UODO w zakresie swojej właściwości na pewno są dodatkowym elementem i niejako uzupełniają to, co w zakresie cyberzagrożeń było poruszane i przedstawiane przede wszystkim przez przedstawicieli NASK i MSWiA. Naszym zdaniem kwestie edukacji i profilaktyki są niezwykle istotne, więc od tego pozwolę sobie zacząć, także w odniesieniu do wcześniejszych wypowiedzi.

Flagowym programem realizowanym przez UODO już od 15 lat jest program „Twoje dane – Twoja sprawa”. Pani minister już o nim wspomniała.

Będę mówić o pewnych datach z uwagi na to, że być może to państwa interesuje. W dniach 22–23 października odbędzie się konferencja szkoleniowa „Prywatność i sztuczna inteligencja w edukacji”.

Przeprowadzamy szkolenia oraz organizujemy spotkania dla uczniów, nauczycieli i rodziców. Każdego roku odbywa się około 5 tys. lekcji i różnorodnych wydarzeń. W każdej edycji bierze udział ponad 50 tys. uczniów, a ponad 5 tys. nauczycieli zostaje zaangażowanych w działania związane z programem.

W programie „Twoje dane – Twoja sprawa” duży nacisk kładziemy na kwestie dotyczące nowoczesnych technologii oraz na ochronę prywatności i danych osobowych, a także na bezpieczne i odpowiedzialne korzystanie z technologii cyfrowych. Są to działania niezwykle potrzebne, które oczywiście wpisują się również w inne działania prowadzone w tym zakresie. Coraz więcej badań, prezentowanych także w Komisji, pokazuje, że młodzi ludzie bardzo dużo czasu spędzają w sieci, ale niekoniecznie znają swoje prawa oraz zasady higieny cyfrowej i ochrony swojej prywatności.

Poza tym projektem, który jest naszym podstawowym programem, współpracujemy także z BRPD. Wspieramy kampanię „Więcej szacunku dla młodego wizerunku”.

Natomiast chciałbym podkreślić, że przykładamy ogromną wagę do kwestii ochrony wizerunku dziecka w internecie. We współpracy z Fundacją Orange UODO wydał poradnik „Wizerunek dziecka w internecie. Publikować czy nie?”. Mam nadzieję, że jest on już dosyć dobrze znany. Wydajemy także inne publikacje, które dodatkowo przygotowaliśmy, dotyczące już bardziej specyficznych obszarów ochrony wizerunku. To materiały dla klubów sportowych, organizacji pozarządowych i placówek oświatowych.

Nie chciałbym się tutaj zbyt chwalić, bo przede wszystkim dobry produkt, który cały czas się rozwija, musi podlegać aktualizacji, ale dosłownie w ubiegłym tygodniu nasz poradnik otrzymał nagrodę w konkursie Global Privacy and Data Protection Awards w kategorii: Edukacja i świadomość. Nagrody zostały przyznane w Seulu przez Global Privacy Assembly (GPA). Myślę zatem, że nasze praktyki są zgodne z tendencjami i trendami światowymi, ale staramy się je upowszechniać także na poziomie lokalnym i regionalnym.

W ramach realizowanego programu UODO rusza w kraj. Natomiast 10 października wspólnie z Krakowskim Szkolnym Ośrodkiem Sportowym i Akademią Kultury Fizycznej w Krakowie organizujemy konferencję dotyczącą ochrony danych osobowych w działalności ośrodków sportowych i różnego rodzaju miejskich ośrodków propagujących kulturę fizyczną. W działaniach urzędu, także nadzorczych, widzimy bowiem, że w różnego rodzaju stowarzyszeniach sportowych i klubach sportowych pojawiają się problemy z ochroną prywatności i wizerunku dziecka. Natomiast oczywiście są to programy, które uzupełniają edukację powszechną.

Tutaj rzeczywiście bardzo chciałbym podziękować ministerstwu i osobiście pani minister Lubnauer, bo spotykaliśmy się i przedstawialiśmy uwagi do nowych projektów w zakresie edukacji zdrowotnej i obywatelskiej. Elementy dotyczące zwalczania cyberprzemocy, hejtu i mowy nienawiści, a związane z rozwojem sztucznej inteligencji, są niezwykle ważnymi elementami tych nowych programów, w których naszym zdaniem warto uczestniczyć.

Proszę pozwolić mi powiedzieć kilka słów o działaniach kontrolnych urzędu, bo oczywiście UODO realizuje działania nadzorcze w ramach kontroli administratorów przetwarzających dane osobowe dzieci. Postanowiłem, że w obecnym roku będzie to jeden z czterech tematów kontroli sektorowych. Kontrole trwały, trwają i będą przeprowadzane. W dużej mierze odnoszą się one zarówno do ochrony danych osobowych, jak i do powiązanych z tym zagadnień cyberodporności czy cyberbezpieczeństwa w placówkach oświatowych.

Incydenty zgłaszane są do nas w kategorii naruszeń i skarg. Rzeczywiście ataki *ransomware* są jednymi z najczęstszych zdarzeń. Naruszenia bezpieczeństwa danych następują z powodu braku procedur, niewystarczającego przeszkolenia pracowników szkoły, wykorzystywania do celów służbowych takich prywatnych zasobów, jak adresy e-mail czy skrzynki pocztowe, zapisywania haseł w przeglądarkach, nieuwagi przy logowaniu, udostępniania dokumentów na publicznie dostępnych platformach i niskiego poziomu wdrażania podstawowych zabezpieczeń. Niestety przyczynia się to także do stwarzania wielu podatności, które potem są wykorzystywane w bardzo negatywnej albo wręcz przestępczej działalności.

Dlatego z naszej perspektywy ważne jest to, co identyfikujemy też w działaniach, jeżeli chodzi o budowanie odporności placówek oświatowych, czyli podnoszenie świadomości kadry szkolnej oraz rodziców, a także wprowadzanie polityk bezpieczeństwa informacji, ograniczanie korzystania z prywatnych narzędzi w szkołach oraz regularne szkolenia z zakresu ochrony danych i cyberhigieny. Wzmocnienie zabezpieczeń technicznych i organizacyjnych na pewno pozwalałoby systemowo ograniczać ryzyko wystąpienia w przyszłości podobnych naruszeń, które niestety się powtarzają.

Chciałbym powiedzieć o pewnych elementach działań legislacyjnych, które może nie były jeszcze podnoszone. Mianowicie UODO przedstawił uwagi zarówno do obywatelskiego projektu

ustawy o ochronie małoletnich, jak i do rządowego projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie. Są to przede wszystkim uwagi w zakresie dotyczącym zapewnienia wieku użytkownika, co miałyby chronić małoletnich przed szkodliwymi treściami. Wskazaliśmy na konieczność wykorzystania oświadczenia Europejskiej Rady Ochrony Danych (EROD), które zawiera zasady zgodnego z prawem przetwarzania danych przy zapewnieniu wieku danej osoby, co jest zgodne z zasadą minimalizacji danych oraz z koniecznością stosowania bezpiecznych i proporcjonalnych mechanizmów weryfikacji. Ten materiał jest oczywiście publicznie dostępny.

Chciałbym zwrócić uwagę na niezwykle ważną rolę, jaką odgrywa wdrożenie rozporządzenia Parlamentu Europejskiego i Rady (UE) w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (eIDAS 2.0). Zresztą rozmawialiśmy o tym wczoraj na spotkaniu w MC. Europejski portfel tożsamości cyfrowej to narzędzie, które może umożliwiać potwierdzanie wybranych atrybutów, na przykład wieku, bez ujawniania pełnych danych osobowych, a przy zapewnieniu ochrony prywatności. W tym zakresie będziemy współpracować z resortem cyfryzacji. Za to też bardzo dziękuję.

Może jeszcze dwie dodatkowe informacje, żeby ograniczyć swoją wypowiedź. Działamy aktywnie w specjalnej grupie do spraw edukacji cyfrowej przy wspomnianej już światowej organizacji GPA. Wspólnie opracowaliśmy tzw. booklet. To broszura, która zawiera około 150 inicjatyw edukacyjnych w obszarze edukacji cyfrowej, realizowanych w ostatnich latach przez kilkadziesiąt organów ochrony danych z całego świata. Broszura była i będzie dystrybuowana w szkołach, przede wszystkim tych biorących udział w programie „Twoje dane – Twoja sprawa”. Zachęcam także do zapoznawania się z nią i sięgania do pomysłów, które tam się znajdują.

Oczywiście planujemy też kontynuację działań na poziomie krajowym, ale po to, żeby wykorzystać nasze możliwości, w kwietniu br. złożyliśmy wniosek o dofinansowanie projektu, który dotyczy przeprowadzenia kampanii edukacyjnej właśnie w zakresie podnoszenia świadomości na temat praw dzieci i ochrony w internecie. To w ramach unijnego programu „Obywatele, równość, prawa i wartości” (CERV). Mamy oczywiście nadzieję, że ten projekt będziemy mogli skutecznie realizować.

Liczę na to, że inicjatywy edukacyjne będą mogły być przez nas dalej realizowane. Bardzo dziękuję, pani przewodnicząca.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Otwieram dyskusję. Czy są chętni do zabrania głosu?

Pan poseł Józefaciuk i pani Katarzyna Szymielewicz. Bardzo proszę zabrać głos w tej kolejności.

Poseł Marcin Józefaciuk (KO) – spoza składu Komisji:

Serdecznie dziękuję.

Szanowna pani przewodnicząca, szanowna pani minister, szanowny panie komendancie, szanowni państwo, po pierwsze, chciałbym podziękować za tematykę obrad Komisji. Musimy sobie na pewno uświadomić, że dzieci i młodzież w internecie tak naprawdę spełniają wszystkie funkcje, a więc są zarówno ofiarami, jak i świadkami, ale również są sprawcami przestępstw. To trzeba mieć na względzie.

Jeżeli chodzi o materiały, to bardzo fajnie został pokryty obszar hejtu i cyberbullyingu. To znaczy, trudno o tym mówić, używając wyrazu „fajnie”. Trochę zabrakło mi natomiast informacji na temat groomingu, który jest coraz bardziej popularny – w cudzysłowie – w internecie, czy też ewentualnie profilaktyki w zakresie zabezpieczenia przed różnymi zabawami typu wyzwania internetowe. To jest niezwykle niebezpieczne, bo przenosi się na plan fizyczny. Dzieciaki nie mają umiejętności rozróżniania, co jest rzeczywistością. W sumie dla nich cyberprzestrzeń jest częścią ich świata rzeczywistego, a nie – tak jak dla nas – jakimś innym światem.

Serdecznie dziękuję za coś fajnego, co wprowadziło MEN w programie „Cyfrowy uczeń”. To jest konieczność stworzenia polityki transformacji cyfrowej w szkole, jak też przeglądu całej polityki cyfrowej. Tak więc dzięki temu będzie można zapewnić, że zostanie to zaktualizowane.

Rzeczywiście NASK bardzo często informowała szkoły, że jest jakiś problem z zabezpieczeniami, ale nie wiem, szczerze mówiąc, na ile było później sprawdzane to, czy dana szkoła zareagowała. Szkoły rzadko kiedy są atakowane, bo wszystkie rzeczy typu dzienniki, system

informacji oświatowej (SIO) i egzaminy są na platformach chmurowych, a nie w szkole. Szkoły nawet już w miarę dobrze zaczynają chronić swoje dane.

Co tak naprawdę jest ważne, a co tutaj nie padło, choć warto by było, żeby padło? Ministrowie cyfryzacji, edukacji czy rozwoju i technologii byli patronami IT Fitness Testu, który w Grupie Wyszehradzkiej sprawdzał umiejętności uczniów i nauczycieli. Byliśmy w nim na szarym końcu. Jeśli chodzi o uzyskanie punktów przez Polskę, to średnia możliwości dla całego kraju wyniosła 46%. Ten test był podzielony na pięć kategorii – internet, cyberbezpieczeństwo, zadania złożone, narzędzia biurowe oraz sieci społecznościowe i cyfrowe narzędzia współpracy. Tutaj mamy bardzo wiele rzeczy do poprawienia, bo rzeczywiście jesteśmy z tyłu i ciągle spadamy. Nie powiem, że w dół, bo to byłby błąd językowy.

Z koleżanką posłanką rozmawialiśmy o tym, że warto się zastanowić, co można byłoby zrobić, bo tutaj bardzo dużo słyszeliśmy o niektórych rzeczach, które są robione, ale znamy stan zastany i tak jakby ciągle nie jesteśmy w stanie się z niego wydostać. Tutaj na pewno przede wszystkim będzie potrzebne duże dofinansowanie edukacji. Chodzi o profesjonalnych informatyków, bo nauczyciel informatyki nie jest informatykiem, tylko nauczycielem informatyki, a bardzo często spełnia funkcję informatyka. Organy prowadzące bardzo rzadko zatrudniają informatyków z prawdziwego zdarzenia po to, żeby chronić dane. Chodzi również o zaopatrzenie w sprzęt. Dzięki pieniądзом z „Krajowego planu odbudowy i zwiększania odporności” (KPO) oraz różnym programom, jak też dzięki MEN i MC, nowoczesny sprzęt – zarówno *hardware*, jak i *software* – jak najbardziej już zaczyna występować, co jest niezwykle ważne.

Serdecznie dziękuję państwu za profilaktykę, bo to jest niezwykle ważne. Profilaktyka musi być jeszcze bardziej celowana. Naprawdę fajnie byłoby dotrzeć do młodzieży, używając młodzieżowego języka, czyli zarówno poprzez influencerów i celebrytów, jak i przez ich sieci. Nie wiem, czy są takie próby.

Oczywiście dzięki eIDAS 2.0 nastąpi próba likwidacji pewnej anonimizacji, co też – że tak powiem – będzie miało pozytywny wpływ na całość. Sytuacja na pewno nie jest superwesola. Mamy wiele rzeczy do zrobienia – zarówno my jako posłowie i jako Sejm, ale też po prostu my jako dorośli. Jest jednak światełko w tunelu i słysząc, że naprawdę te rzeczy zaczynają przynosić oczekiwane sukcesy.

Tak więc serdecznie dziękuję. Raz jeszcze dziękuję za tematykę obrad Komisji.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Pani Katarzyna Szymielewicz z Fundacji Panoptykon.

Prezes Fundacji Panoptykon Katarzyna Szymielewicz:

Pani przewodnicząca, dziękuję za zaproszenie i za udzielenie głosu. Dziękuję też przedmówcom za zarysowanie ważnych działań. Podpisuję się pod poprzednim głosem. To prawda, że prewencja i profilaktyka są szalenie ważne. Bardzo dobrze jest słyszeć, że jako państwo robimy tak dużo. Niemniej jednak tym, na co chcę zwrócić uwagę, są zagrożenia, na które państwo ma ograniczony wpływ, bo dzieją się w tym miejscu, gdzie państwa i instytucji nie ma, czyli w sieci, a szczególnie w sieciach społecznościowych.

Dziś odbywa się drugi dzień konferencji „Safer Internet” pod patronatem pani minister edukacji, ministra cyfryzacji i rzecznika praw dziecka. Jest to wspaniała konferencja, na której miałam okazję dzisiaj występować. W tym roku w zasadzie cała jej tematyka jest poświęcona doświadczeniom dzieci w sieciach społecznościowych.

Fundacja Dajemy Dzieciom Siłę, która jest organizatorem tej konferencji i od 19 lat ją prowadzi, zaczęła właśnie kampanię „15+ powodów”, aby podnieść próg wejścia do mediów społecznościowych. Wśród 15 powodów znajdują państwo porażającą listę zagrożeń – od uzależnień i cyberprzemocy, przez pornografię, wykorzystanie seksualne i uwodzenie, po problemy ze zdrowiem psychicznym i samooceną, lęk przed wypadnięciem z obiegu (FOMO), narażenie na stres, problemy z koncentracją itd.

Oczywiście te problemy, choć w inny sposób i innymi słowami, dostrzega również Komisja Europejska. Mamy cały czas dość świeżą w Polsce, a szalenie ważną regulację. Zaraz o niej wspomnę. Dlaczego właśnie dzisiaj o niej wspominam? To akt o usługach cyfrowych (DSA), gdzie z kolei mamy obowiązek, żeby wielkie platformy przynajmniej raz w roku spowiadały się ze swoich grzechów głównych. Tam jest podobna lista zagrożeń, które te platformy powinny

dokumentować i im zapobiegać. Raporty z ubiegłego roku, jeśli chodzi o rodzaje ryzyka dla dzieci, były słabe. To jest bardzo dyplomatyczne określanie. Badania, do których mamy dostęp w Polsce, pokazują o wiele więcej, niż pokazały platformy. Zobaczmy, co pokażą one tej zimy, ale to nie jest tak, że na te zagrożenia możemy patrzeć z boku i czekać, aż naprawią je czy zaradzą im ci, którzy zarabiają na eksploatacji danych, prywatności, uwadze i emocjach dzieci.

Dzięki danym, które publikują m.in. Fundacja Dajemy Dzieciom Siłę i inne organizacje, wiemy, że skala tego problemu w Polsce jest porażająca. Przywołam tutaj tylko świeże dane, które pokazywano właśnie na wspomnianej konferencji. Mówimy o 1,5 mln dzieci poniżej 13. roku życia, które są w sieciach, a więc to jest naprawdę duża liczba. Mówimy o tym, że 50% nastolatków korzysta z portali społecznościowych jako źródła informacji, a szczególnie jako inspiracji do tego, jak powinny wyglądać i się zachowywać. Mówimy o tym, że 43% nastolatków korzysta z tych mediów, żeby poczuć się lepiej, czyli idą tam po to, żeby nie być same, ponieważ już cierpią i doświadczają stresu, a nie mają z kim – czy to w domu, czy to w szkole – się podzielić, ale w efekcie wejścia do tych sieci jest coraz gorzej.

Na to mamy akurat bardzo twarde dane i z zagranicy, i z Polski. Od 20 lat sieć Health Behaviour in School-aged Children (HBSC) zbiera dane o zdrowiu nastolatków. Polskie pikują. Szczególnie 13-letnie dziewczyny są bardzo narażone na problemy psychiczne, a jedna piąta już 2 lata temu raportowała przejawy uzależnienia i FOMO. Fundacja Dajemy Dzieciom Siłę pokazuje dane, zgodnie z którymi połowa nastolatków deklaruje niski poziom samooceny, alienację itd. Naprawdę więc nie jest dobrze.

Zadam dziś pytanie. Co z polskiej perspektywy możemy z tym zrobić? Akt o usługach cyfrowych to jest oczywiście regulacja europejska, którą przede wszystkim egzekwuje Komisja Europejska. Otóż możemy zrobić tyle, że w Polsce można wdrożyć ten akt. To jest kwestia tego tygodnia. Projekt znajduje się już w Radzie Ministrów.

Dzisiaj w mediach znowu słyszymy głosy i zarzuty pod kątem tej regulacji, jakoby była ona zarzewiem cenzury. W mojej ocenie jest to po prostu dezinformacja, i to często podlewana albo z Rosji, albo z USA. My jako obywatele, a państwo jako decydenci powinniśmy przeciwstawiać się dezinformacji na temat regulacji, która w Polsce naprawdę może mieć pozytywne znaczenie nawet dla tego obszaru, o którym tu rozmawiamy.

W Polsce kompetencje dalej pozostaną przy starym i jednocześnie nowym urzędzie, czyli Urzędzie Komunikacji Elektronicznej. Właśnie w innym budynku Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii zaopiniowała pozytywnie kandydaturę Przemysława Kuny, który ma doświadczenie z NASK, gdzie zarządzał projektami edukacyjnymi. Myślę, że to będzie sojusznik w tym, żeby tematykę portali społecznościowych traktować w Polsce poważnie.

Ostatnia myśl. Wiem, że Komisja ma przed sobą pracę nad ustawą o tzw. zakazie telefonów w szkołach, gdzie bardzo pośrednio ten temat jest traktowany. Bardzo bym chciała, żebyśmy mogli o tym podyskutować na dedykowanym posiedzeniu, ponieważ ten środek nie zbiera dobrych recenzji. Szczególnie na konferencji „Safer Internet”, gdzie cała sala była wypełniona pedagogami i osobami ze szkół, ustawa zbierała fatalne recenzje. Jeżeli poprzestaniemy na tak powierzchownym środku, być może nawet nieskutecznym albo szkodliwym, to popełnimy ogromny błąd. To jest zdanie pedagogów, a nie moje, bo nie mam nawet kompetencji, żeby to oceniać.

Zdaniem pedagogów być może stracimy szansę, żeby poważnie zająć się tematyką wchodzenia przez dzieci w media społecznościowe. Trzeba pomyśleć, jak możemy pomagać im stamtąd wychodzić, na przykład wzmacniając je psychicznie, budując ich odporność i kompetencje medialne od przedszkola, a nie dopiero na późniejszym etapie, zamiast kłaść nacisk na kompetencje cyfrowe, które są straszną pułapką.

Tu akurat żałuję, że się nie udało, bo choćby w Radzie do Spraw Cyfryzacji próbowaliśmy zamienić termin „kompetencje cyfrowe” na „kompetencje medialne” i położyć nacisk na fundamentalne rzeczy, jakimi są etyczne myślenie, odporność psychiczna czy czytanie tekstu. Nie udało się jednak tego osiągnąć. Wbrew temu, że Organizacja Współpracy Gospodarczej i Rozwoju (OECD) posługuje się przecież słowami „*core literacy*”, a nie „kompetencje cyfrowe”, Polska dalej mówi „cyfrowe, cyfrowe, cyfrowe”, co powoduje zły PR tych kompetencji. Nauczyciele klas I–III myślą, że cyfrowość oznacza komputer na lekcji i klikanie. Nie myślą tak, jak my tego byśmy chcieli – że ich rolą jest wesprzeć dzieci, zanim trafią do sieci, żeby myślały krytycznie. To zatem sygnalizuję.

Pani minister, może jeszcze jest jakaś szansa, żeby w materiałach dla nauczycieli położyć nacisk na kompetencje medialne i *core literacy*, a nie kompetencje cyfrowe, które dziś brzmią jak z innej epoki i jak problem, a nie jak obietnica? Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Dziękuję.

Czy są jeszcze jakieś zgłoszenia z sali?

Jeśli nie, to pozwolę sobie zadać pytanie, bo pani Katarzyna Szymielewicz powiedziała o dezinformacji. Mam więc pytanie. Czy państwo obserwują zorganizowane działania na rzecz dezinformacji w Polsce? Chodzi o wykorzystywanie platform cyfrowych do tego, aby siać panikę, niepokój, chaos i kłamstwa, powielać jakieś rzeczy, które – nie wiem – wpływają na przykład na polityki publiczne. W sytuacjach kryzysowych dezinformacja wpływa na to, jakie informacje pojawiają się w mediach. Szczególnie osoby młode, niemające jeszcze wykształconego krytycznego myślenia, są podatne na takie informacje i ulegają manipulacjom.

Dzisiaj doszło do aresztowania czwartego już dziesiętnastolatka z Olsztyna podejrzanego o terroryzm czy o przygotowywanie ataku terrorystycznego. Czy te osoby komunikowały się przez internet i przez media społecznościowe? Czy państwo to widzą? Jeśli tak, jaka to jest skala? Skąd pochodzą takie ataki, jeśli chodzi właśnie o kwestię rekrutacji młodych osób i ich radykalizację, ale także o kwestię siania dezinformacji i chaosu w społeczeństwie?

Zastępca komendanta CBZC insp. Bartosz Furgała:

Szanowna pani przewodnicząca, jako CBZC zajmujemy się zagadnieniami, które muszą wypełniać znamiona przestępstwa. Natomiast oczywiście przy wielu różnych zdarzeniach, które są istotne dla funkcjonowania naszego państwa, jak i w różnych obszarach widzimy bardzo wzmożoną aktywność dezinformacyjną. Pochodzi ona tak naprawdę głównie z kierunku wschodniego – czy to białoruskiego, czy też rosyjskiego. Najlepszym tego przykładem jest ostatnia sytuacja związana z atakiem dronów czy też tym momentem, kiedy naruszona została polska przestrzeń powietrzna.

Skala dezinformacji jest niepoliczalna. Ona jest olbrzymia. Tym, co możemy zrobić w tym zakresie, jest monitorowanie treści, które się pojawiają w mediach społecznościowych i w komentarzach, co oczywiście robimy. Przekazujemy je do Ośrodka Analizy Dezinformacji NASK. Występujemy również do operatorów o to, żeby zgodnie z ich regulaminami usuwać poszczególne treści.

Natomiast w mojej ocenie to są cały czas czynności nie do końca skuteczne z uwagi na brak wystarczających możliwości prawnych. Wierzę, że to, o czym mówiliśmy, czyli implementacja DSA i nowe rozwiązania, pozwolą na skuteczniejszą walkę, jeśli chodzi o dezinformację.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Czy MEN chce się odnieść? Bardzo proszę.

Sekretarz stanu w MEN Katarzyna Lubnauer:

Tak. Chciałabym się odnieść do pana wypowiedzi. Po pierwsze jako matematyk chciałabym powiedzieć, że to jednak jest policzalne. Tego jest dużo, ale jest policzalne. To jest już jednak – że tak powiem – moje zboczenie zawodowe.

Natomiast w kwestii edukacji chcemy przede wszystkim wprowadzić jedną rzecz. Chodzi o to, żeby przedszkola były przestrzenią wolną od ekranów i od cyfryzacji. Uważamy, że to jest taki wiek, w którym musimy dokładnie uzupełniać braki wynikające z faktu, że często dziecko bardzo wcześnie dostaje tablet lub telefon do ręki. Powiem, że ostatnio na jednym ze spotkań, gdzie otwieraliśmy jakąś instytucję szkolną, byłam obserwatorem pewnej sceny. Dziecko w wózku i to jeszcze ze smoczkiem – na moje oko miało jakieś dwa lata – całą uroczystość, która całkiem sporo trwała, siedziało z tabletem w ręku, oglądając jakieś migające obrazki.

Muszę powiedzieć, że zależy nam na tym, żeby przedszkole było miejscem, w którym dzieci uczą się tego świata. Jeżeli mówimy o cyberbezpieczeństwie, to w tym znaczeniu, że w ramach zwracania im uwagi, jak się zachowujemy w niektórych przestrzeniach – że na przykład przy jedzeniu nie możemy siedzieć z telefonem itd. Natomiast chodzi o przestrzeń bez ekranów, dlatego że mamy bardzo dużo rzeczy do nadrobienia, takich jak na przykład zdolności manualne, kwestia aktywności fizycznej czy sprawa takiego zwykłego bycia ze sobą. Nauczyciele wskazują,

że zdolności manualne są dużo mniejsze. Teraz mamy pokolenie jedynaków, w związku z czym bardzo często dzieci mają mniejsze umiejętności społeczne. To jest kwestia – że tak powiem – działania w grupie, ale też kreatywności. Jest jeszcze rzecz, która niestety chyba będzie największą plagą w przyszłości, zwłaszcza w szkole. Chodzi o brak uważności, czyli skupienia, której to umiejętności bardzo często niestety pozbawiają nas komórka, tablet i inne tego typu media.

Natomiast w klasach I–III oczywiście musimy być bardzo oszczędni. To znaczy, rzeczywiście szcycimy się tym, że dość wcześnie mamy wiedzę informatyczną, ale coraz bardziej zdajemy sobie sprawę z zagrożeń. Znamy też raport „Internet dzieci”. Widzimy, co tam się dzieje. Natomiast cały czas mamy takie poczucie, że wielu osobom, które patrzą na to z zewnątrz, wydaje się, że jak zabronimy korzystania z komórek w szkole, to rozwiążemy problem. Musimy jednak pamiętać chociażby o tym raporcie, że to jest na 4,5 godziny, więc bardziej chodzi tu o profilaktykę polegającą na edukacji.

Dlatego szkoda, że jednak tak wielu rodziców nie decyduje się na to, żeby ich dziecko chodziło na edukację zdrowotną, bo dokładnie tego typu przedmiot jest miejscem, gdzie dzieci mogą się dowiedzieć o groomingu, o którym tu pytał pan poseł, o sextingu, o cyberbezpieczeństwie i o zagrożeniach, których często nie znali ich rodzice, w związku z czym nie są w stanie ich tego nauczyć. Na zajęciach uczniowie dowiedzą się również tego, czym jest higiena cyfrowa.

Oczywiście nie jest tak, że kiedy młodych ludzi tego uczymy, to każdy z nich podaży za wytycznymi, ale przynajmniej część z nich przekazuje to rodzicom. To jest też pewna recepta. Tak jak kiedyś dzieci uczące się segregacji śmieci nauczyły tej procedury swoich rodziców, tak teraz dzieci uczące się o cyberbezpieczeństwie bardzo często przynoszą tę wiedzę do domów i uczulają na to swoich rodziców, którzy potem mają szansę zwracać uwagę na to, że fakt, iż są sami w pokoju, nie oznacza, że są bezpieczni. To jest zresztą słynna scena z miniseriale „Dojrzewanie”, gdzie rodzice byli głęboko przekonani, że ponieważ ich syn jest w pokoju gdzieś tam w domu, to w związku z tym jest bezpieczny, a okazało się zupełnie inaczej.

Dlatego na pewno we wszystkich działaniach profilaktycznych będziemy na to bardzo silnie zwracać uwagę. Stąd wszędzie pojawiają się te elementy, o których mówimy przy okazji edukacji medialnej – i w edukacji obywatelskiej, i w edukacji zdrowotnej. Uważamy, że praktycznie w każdej z tych przestrzeni warto mówić młodzieży o tym, jakie są zagrożenia. Stąd wspólnie z UODO współpracujemy przy projekcie „Twoje dane – Twoja sprawa”, dlatego że uważamy, iż tego typu konkursy, w których często młodzież przygotowuje wiedzę dla reszty młodzieży, są ważne, ponieważ wtedy uczniowie są w to bardziej zaangażowani.

Przewodnicząca poseł Monika Rosa (KO):

Tak.

To jeszcze zbiorę zgłoszenia. Czy pani Katarzyna Hernandez się zgłasza? Nie. Bardzo proszę. Za chwilę oddam głos pani Katarzynie Szymielewicz.

Członek Rady Młodzieżowej przy Parlamentarnym Zespole do spraw Młodzieży Nikita Pavlenco:

Dzień dobry. Nikita Pavlenco, Rada Młodzieżowa przy Parlamentarnym Zespole do spraw Młodzieży.

Kiedy mówimy o cyberbezpieczeństwie dzieci i młodzieży, to przede wszystkim wiadomo, że najpierw wchodzi zagrożenia w postaci cyberprzemocy, hejtu, wyłudzeń i phishingu, ale moim zdaniem trzeba też zwracać uwagę na takie nowe zagrożenia, jak technologia *deepfake*. Narzędzie, które jeszcze kilka lat temu wydawało się futurystycznym eksperymentem, dziś po prostu staje się powszechnie dostępne. Dzięki sztucznej inteligencji w kilka minut można stworzyć fałszywy obraz czy nagranie, które są pozornie autentyczne, a w rzeczywistości po prostu zmanipulowane.

Moje pytanie skierowane jest do MEN i do MC. Czy są planowane konkretne działania, aby chronić dzieci i młodzież przed nadużyciami, które są związane z treścią generowaną przez sztuczną inteligencję? Czy możemy oczekiwać jakichś systemowych rozwiązań w edukacji, uczących właśnie krytycznego myślenia i rozpoznawania manipulacji, a także w zakresie narzędzi technicznych do weryfikacji fałszywych materiałów?

Moim zdaniem to jest właśnie ten moment, w którym musimy myśleć o przyszłości dzieci, bo jeśli dziś nie przygotujemy tych skutecznych mechanizmów obrony, to jutro może być po prostu za późno. Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Dziękuję.

Jeszcze pani Katarzyna Szymielewicz, a potem zamykam już dyskusję. Jeśli któryś z przedstawicieli resortów chciałby odpowiedzieć, to bardzo proszę.

Prezes Fundacji Panoptykon Katarzyna Szymielewicz:

Dziękuję bardzo. *Ad vocem* trzy rzeczy.

Jeśli chodzi o policzalność dezinformacji, to osobiście znam ekspertów, którzy liczyli nawet tę ostatnią falę. To jest oczywiście kwestia dostępu do odpowiednich narzędzi i danych. Takie narzędzia wielkie platformy muszą wystawiać badaczom. Mam nadzieję, że w Polsce ta procedura też lada moment zacznie działać dzięki wdrożeniu DSA, o którym to akcie już mówiliśmy, więc badacze certyfikowani do tego celu będą mieli bezpośredni dostęp do różnych danych. Nawet dzisiaj jednak są organizacje, które de facto mają dostęp do tych interfejsów. Wśród nich są też polskie organizacje. Pojawiały się więc raporty, choć rzeczywiście nie ze strony NASK.

To jest taki moment, w którym czuję dysonans poznawczy. Skoro mam dostęp do tego typu danych albo mogłabym mieć, gdybym chciała, to jakim cudem najbardziej kompetentne organy w Polsce, które powinny to widzieć i reagować, takiego dostępu nie mają? Coś tutaj nie gra. Na pewno nie jest to temat obrad Komisji, ale może na jakimś innym posiedzeniu powinniśmy się zastanowić nad tym, jak spowodować, by ta sieć działała razem i wzmacniała się, a nie zwalczała.

Jeśli chodzi o ocenę programową, to miałam przyjemność recenzować nowy profil i podstawę informatyczną. Widziałam w nich naprawdę bardzo dużo nowego myślenia. Tutaj czapki z głów – przed Instytutem Badań Edukacyjnych (IBE) za odwagę, i przed panią minister za to, że przyjęliście ten kierunek. Natomiast ludzie, z którymi rozmawiam – czy na konferencji „Safer Internet”, czy w podobnych kręgach – wyrażają obawy, że to się potem rozbija nawet nie o nauczycieli, tylko o ostatnią milę, czyli o materiały dydaktyczne, które tworzą zwykle inne osoby. Podobno przekazują...

Sekretarz stanu w MEN Katarzyna Lubnauer:

Spokojnie. My to nadzorujemy. Pojawi się nawet recenzja metodyczna. Rzeczywiście zmieniamy podejście do podręczników. Co więcej, jesteśmy w ścisłej współpracy również z wydawcami w czasie całego procesu tworzenia podstaw programowych i tego podejścia. Nie chcę reklamować wydawnictwa, ale muszę powiedzieć, że na przykład po jednym z podręczników do edukacji obywatelskiej już widać, w jak dużym stopniu są w nim uwzględnione wszystkie uwagi dotyczące tego, co tam się powinno znaleźć. W związku z tym staramy się też zmienić podejście do kwestii współpracy z wydawcami.

Prezes Fundacji Panoptykon Katarzyna Szymielewicz:

To wspaniale. Bardzo mocno trzymamy kciuki. Jeżeli jest taka chęć w ministerstwie, to na pewno ucieszą się eksperci z tych wszystkich konferencji i gremiów, które państwo wspierają jako ministerstwa i instytucje. Tam jest ogrom wiedzy, materiałów i doświadczenia, jak uczyć pewnych rzeczy. Myślę, że nawet włączenie ich – czy w trybie recenzji, czy w trybie jakiegoś omawiania tego – pozwoliłoby nam docierać...

Sekretarz stanu w MEN Katarzyna Lubnauer:

Niech się zgłaszają do zespołu recenzentów. Ministerstwo Edukacji Narodowej przyjmuje recenzentów podręczników. Różne organizacje, które zajmują się badaniami czy inną działalnością tylko w tej dziedzinie, mogą zgłaszać.

Prezes Fundacji Panoptykon Katarzyna Szymielewicz:

Dobrze. Myślałam, że jest odwrotnie i to IBE musi przyjść do nich. Jeżeli możemy się zgłaszać, to rozpuszczę takie wici.

Zmierzam do ostatniej uwagi *ad vocem*, bo à propos edukacji zdrowotnej wszyscy ubolewamy, że ona nie będzie obowiązkowa. Może jednak jest jeszcze szansa na zrobienie jakiejś kampanii? Wyszedł już poseł influencer, ale może właśnie to jest ta droga, żeby osoby, które mają zasięgi, a są z różnych stron polskiej debaty publicznej, mówiły o wartości tego przedmiotu, używając przeróżnych argumentów. Dezinformacja, odporność psychiczna czy kompetencje medialne to są naprawdę świetne przykłady, którymi można byłoby się posługiwać, żeby odchodzić od tego, co niesłusznie wywołało kontrowersje.

Znowu mam apel do MEN czy do rzecznika. Może nie oddawajmy jeszcze tego pola? Rozumiem, że w tym roku karty są już trochę rozłożone czy rozdane, ale może pieniądze publiczne plus zaangażowanie odpowiednich osób mogą jednak spowodować przekonanie rodziców, żeby dzieciaki na te zajęcia zaczęły chodzić. Wydaje mi się bowiem, że będzie bardzo źle, jeżeli stracimy szansę na te zajęcia, jeżeli tutaj znowu oddamy pole de facto dezinformacji. Dziękuję.

Poseł Barbara Okuła (Polska2050-TD):

Tak króciutko na podsumowanie chciałabym też właśnie podziękować za zorganizowanie obrad Komisji na ten temat, bo myślę, że jest to bardzo ważny temat.

Chciałabym też nawiązać do dezinformacji. Mam takie wrażenie, że ostatnio trudno się przebić z informacją czy z prawdą przez dezinformację, która jest w sieci, ale też i w mediach. Tak samo jest właśnie z edukacją zdrowotną. Naprawdę trudno jest przekonać rodziców, pokazać im coś i przebić się przez tę dezinformację, która jest.

Jeśli chodzi o dzieci w sieci, to wydaje mi się, że musimy przede wszystkim trafić do rodziców, bo nawet zakaz używania telefonów komórkowych w szkole nie rozwiąże nam problemu, kiedy dzieci, wracając ze szkoły do domu, siedzą w telefonach, z których często właśnie czerpią tę dezinformację. Musimy uświadamiać rodziców, z jakich stron dzieci powinny korzystać. Zdaje mi się, że tutaj ważna jest praca nad rodzicami, którzy często żyją w nieświadomości i nie wiedzą, że jest coś takiego jak kontrola rodzicielska, że mogą skorzystać z programów, które też będą to kontrolowały, jeśli oni sami nie są w stanie być z dzieckiem i sprawdzać, bo jeśli ten problem będzie narastał... Tak jak widzimy, statystyki rosną. Coraz trudniej będzie wyrwać dzieci ze świata internetowego, bo one faktycznie często uciekają w ten świat i w nim właśnie żyją. Dziękuję bardzo.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Jeszcze pan prezes Wróblewski i pani Katarzyna Hernandez z BRPD.

Prezes UODO Mirosław Wróblewski:

Bardzo dziękuję, pani przewodnicząca.

Krótko chciałbym się odnieść do problemu, który został przez pana podniesiony. *Deepfake* to jest rzeczywiście poważny problem. Różnymi metodami w zakresie kompetencji urzędu staramy się ten temat podejmować. W ubiegłym roku dwukrotnie ograniczyłem przetwarzanie danych osobowych dla platformy Meta, natomiast z uwagi na właściwość organu irlandzkiego postępowanie jest tam prowadzone. Przyczyniło się to jednakże do szerszego dialogu z platformą. Chodzi o zjawisko *celeb bait*. Dla osób, które są pokrzywdzone czy czują się ofiarami tego typu działalności, Meta uruchomiła kanał, gdzie jest możliwość zgłaszania treści o charakterze *deepfake* czy *scam*. Trzeba więc stosować środki represyjne, jak też uczestniczyć w rozmowach, co staramy się robić.

Natomiast rzeczywiście są to kwestie bardzo negatywne dla wielu uczniów, także na przykład w kontekście wykorzystywania do tworzenia pornografii. Muszę powiedzieć, że miałem okazję złożyć zawiadomienia do organów ścigania, choć na razie bez większych sukcesów, więc będziemy... Powiedziałbym, że także w tym względzie prowadzimy postępowania o różnym charakterze procesowym.

Dodam jeszcze tylko ostatnią rzecz, że przeprowadziliśmy analizę rozwiązań europejskich przyjmowanych w poszczególnych krajach, bo rzeczywiście pojawia się ich coraz więcej. Poprosiliśmy tutaj o współpracę ministra cyfryzacji. Chodzi o rozważenie konieczności stworzenia krajowej regulacji, która uzupełniłaby wszystkie dotychczasowe przepisy, w tym także europejskie. Jesteśmy gotowi do współpracy, jeżeli będzie tylko taka możliwość. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Bardzo proszę, pani Katarzyna Hernandez.

Dyrektor Zespołu Edukacji Cyfrowej i Bezpieczeństwa w Sieci Biura Rzecznika Praw Dziecka Katarzyna Hernandez:

Szanowni państwo, szanowna pani przewodnicząca, również przede wszystkim chciałabym podziękować, bo nigdy za dużo rozmowy na temat bezpieczeństwa dzieci w sieci. To jest jedna rzecz.

Druga rzecz dotyczy tematu cyberbezpieczeństwa młodych. W dzisiejszych czasach tak naprawdę to jest po prostu kluczowa sprawa, bo wszyscy tutaj obecni wiedzą, co się dzieje w sieci. Do BRPD wpływa bardzo dużo zgłoszeń, i to nie od dorosłych, tylko od młodych osób, które bardzo często są pokrzywdzone w sieci, gdzie w jakiś sposób doświadczają cyberprzemocy i hejtu. Właśnie te młode osoby proszą nas o to, żebyśmy mimo wszystko nie zabraniali im dostępu do nowych technologii, a raczej wchodzili w taką narrację, żeby środowisko cyfrowej rzeczywistości było dla nich jak najbardziej bezpieczne.

W ogóle cieszę się, że mamy tutaj przedstawicieli młodych osób, natomiast chciałabym też trochę zaapelować o to, żebyśmy nie zapominali o ich głosie, tworząc programy, przedmioty i projekty edukacyjne dla młodych osób. Nie zapominajmy o tym, że to oni są tymi osobami, które spędzają godziny w sieci, co pokazują badania. Tak naprawdę młodzi ludzie mogą być niezwykle cennym źródłem wiedzy o tym, co się dzieje, tak żeby podręczniki i materiały były po prostu aktualne oraz odpowiadały na ich potrzeby i obecne wyzwania.

Deklaruję też wsparcie BRPD dla wszelkich działań, jakie będą tutaj podejmowane. Bardzo dziękuję.

Przewodnicząca poseł Monika Rosa (KO):

Bardzo dziękuję.

Czy któryś z przedstawicieli resortów chciałby zabrać głos?

Jeśli nie, to bardzo państwu dziękuję za uczestnictwo w obradach Komisji.

Zastanowimy się nad tym, czy do poszczególnych resortów będziemy jeszcze wysyłać jakieś wnioski, zapytania albo sugestie.

Bardzo dziękuję. Zamykam posiedzenie Komisji.