

W siedzibie Najwyższej Izby Kontroli 8 lipca odbył się panel ekspercki pn. „Bezpieczne dziecko w świecie cyfrowym – systemowe rozwiązania, wspólna odpowiedzialność”. Efektem debaty są wnioski zebrane w dokumencie porządkującym najważniejsze konkluzje i propozycje działań przedstawione przez ekspertów zajmujących się bezpieczeństwem dzieci i młodzieży w internecie – reprezentantów administracji publicznej, środowiska naukowego, wymiaru sprawiedliwości, oświaty, policji i organizacji pozarządowych.

Intencją Najwyższej Izby Kontroli jest, aby wnioski te stanowiły punkt odniesienia dla dalszych prac nad wzmacnianiem systemu ochrony dzieci i młodzieży w internecie. Ich wdrażanie może przyczynić się do zwiększenia odpowiedzialności instytucji publicznych, sektora technologicznego, szkół, rodziców i opiekunów za bezpieczeństwo najmłodszych użytkowników sieci, a tym samym do skuteczniejszego przeciwdziałania zagrożeniom w świecie cyfrowym.

Dokument został wypracowany wspólnie przez Najwyższą Izbę Kontroli, Kancelarię Premiera, Kancelarię Prezydenta, Ministerstwo Cyfryzacji, Ministerstwo Edukacji Narodowej, Ministerstwo Sprawiedliwości i Biuro Rzeczniczki Praw Dziecka.

Wnioski uczestników panelu ekspertów w NIK

Wobec rosnącej skali zagrożeń, wynikających z dynamicznego rozwoju rynku usług cyfrowych, obejmujących m.in. niekontrolowany dostęp do potencjalnie szkodliwych treści, nawiązywanie niebezpiecznych kontaktów, ryzyko wykorzystywania seksualnego, cyberprzemocy oraz uzależnień, uznajemy, że ochrona dzieci i młodzieży w środowisku cyfrowym wymagają skoordynowanych i systemowych działań. Ich skuteczność oznacza konieczność połączenia regulacji, edukacji, profilaktyki oraz wdrażania realnych mechanizmów egzekwowania przyjętych standardów.

Odpowiedzialność za bezpieczeństwo dzieci spoczywa solidarnie na państwie, instytucjach publicznych, szkołach, rodzicach, organizacjach społecznych oraz dostawcach usług cyfrowych.

Wspólne wnioski z dyskusji obejmują:

Wzmocnienie skoordynowanej współpracy międzyinstytucjonalnej i międzysektorowej na rzecz bezpieczeństwa dzieci w internecie.

Skala i złożoność zagrożeń cyfrowych przekraczają możliwości przeciwdziałania im przez pojedyncze instytucje, dlatego konieczne jest budowanie trwałych mechanizmów współdziałania administracji, wymiaru sprawiedliwości, systemu edukacji, pomocy społecznej, organizacji społecznych, regulatorów rynku cyfrowego oraz rodziców i opiekunów. Jedynie podejście oparte na wspólnych standardach, wymianie informacji i regularnej ocenie skuteczności wdrożonych rozwiązań może przełożyć się na realną ochronę i prewencję adekwatną do dynamiki oraz skali zagrożeń.

Wzmocnienie roli rodziców w procesie zapewnienia bezpieczeństwa dzieci w sieci – zbudowanie świadomości i poczucia odpowiedzialności w rodzinie.

Konieczność zmiany podejścia z reaktywnego na proaktywne. Kluczem do wdrożenia tego modelu jest stworzenie w domu atmosfery zaufania, w której bezpieczeństwo nie kojarzy się z zakazami, a ze świadomym wyborem. Budowanie bezpieczeństwa w rodzinie opiera się na otwartej komunikacji, gdzie

dziecko wie, że może przyjść z każdym problemem, bez strachu. Ważna jest rola rodzica jako „cyfrowego przewodnika”, który zamiast tylko blokować dostęp do internetu, rozmawia o ryzykach sieciowych i wspólnie z dzieckiem ustala jasne limity. Równolegle należy wdrażać trening asertywności w relacjach z rówieśnikami oraz nieznanymi. Pamiętać należy, że wszystkie te elementy zadziałają jednak w sytuacji, gdy przykład idzie z góry. Dzieci najszybciej przejmują zdrowe nawyki, obserwując codzienne zachowania swoich rodziców.

Wyeliminowanie dostępu dzieci do pornografii i treści nielegalnych oraz zdecydowane ograniczenie dostępu do innych treści szkodliwych i niebezpiecznych, a także wzmacnianie ochrony prywatności i wizerunku dziecka.

Nieograniczona, nieuświadomiona i pozbawiona kontroli ekspozycja na treści nieadekwatne do wieku może mieć poważne konsekwencje dla bezpieczeństwa, zdrowia psychicznego i relacyjnego dzieci – to bezdyskusyjny fakt. Zatem konieczne jest możliwie pilne wypracowanie oraz wdrożenie skutecznych rozwiązań prawnych, technicznych i edukacyjnych, które ograniczą ten dostęp. Jednocześnie należy systemowo chronić prywatność i wizerunek małoletnich, w tym przeciwdziałać praktykom nadmiernego upubliczniania ich danych i wizerunku w przestrzeni cyfrowej (tzw. sharenting).

Wprowadzenie jasnych, jednolitych i praktycznych standardów reagowania na zagrożenia cyfrowe wobec dzieci.

Brak czytelnych procedur zwiększa ryzyko podejmowania opóźnionych i niespójnych decyzji oraz wtórnego skrzywdzenia dziecka. Z tego względu każda osoba, podmiot, instytucja (w tym szkoła i placówka) pracująca z dziećmi powinna dysponować narzędziami i przejrzystymi mechanizmami reagowania na cyberprzemoc, grooming, seksting, publikację kompromitujących materiałów oraz inne zagrożenia i formy krzywdzenia online. Powinny być one spójne ze Standardami Ochrony Małoletnich i powiązane z praktycznymi działaniami profilaktycznymi, diagnostycznymi i interwencyjnymi oraz uwzględniać głos dzieci i młodzieży.

Wsparcie dla kompleksowej edukacji cyfrowej w systemie oświaty oraz zwiększanie świadomości i wsparcie nauczycieli, rodziców i opiekunów.

Kompetencje cyfrowe, znajomość zasad higieny cyfrowej, umiejętność krytycznego i twórczego wykorzystania narzędzi sztucznej inteligencji, budowanie świadomości dot. konsekwencji korzystania z narzędzi cyfrowych oraz umiejętne i wczesne rozpoznawanie zagrożeń powinny być rozwijane od najwcześniejszych etapów edukacji w sposób spójny, stopniowy i dostosowany do wieku dziecka. Każdy użytkownik internetu powinien być wyposażony w kompetencje cyfrowe, rozumiane nie tylko jako umiejętność korzystania z technologii cyfrowych, ale również zdolność do krytycznej oceny źródeł, weryfikacji faktów oraz rozpoznawania dezinformacji i manipulacji (np. fake news, deepfake) w internecie. Konieczne są również wczesne edukowanie w zakresie ścieżek reagowania na ryzykowne treści i budowanie zaufania do dorosłych i instytucji. Skuteczność tych działań zależy jednocześnie od właściwego przygotowania nauczycieli oraz włączenia rodziców i opiekunów w działania edukacyjne i profilaktyczne, zwiększenia ich świadomości i czujności, podkreślania ich odpowiedzialności, tak aby przekaz wychowawczy był konsekwentny i wzajemnie wzmacniający. W oczywisty sposób wymaga to zaangażowania nauczycieli, rodziców i opiekunów w codzienną tzw. pozytywną profilaktykę zagrożeń cyfrowych. Równie istotna, o ile nie fundamentalna, jest przy tym powszechność oraz dostępność oferty stanowiącej jakościową alternatywę dla smartfonów, internetu, social mediów, tj. zapewnienie warunków

dla aktywności offline – z dala od ekranu, w bezpośrednim i integrującym kontakcie z rówieśnikami.

Zwiększenie realnej odpowiedzialności dostawców usług cyfrowych za bezpieczeństwo małoletnich.

Ochrona dzieci nie może bazować wyłącznie na indywidualnej ostrożności użytkowników, ponieważ poziom ryzyka w dużej mierze kształtują rozwiązania projektowe, algorytmiczne i organizacyjne, stosowane przez międzynarodowe platformy cyfrowe. Konieczne jest zatem konsekwentne wdrażanie i egzekwowanie przepisów regulujących ten obszar oraz rozwijanie bezpiecznego projektowania usług, skutecznej moderacji treści szkodliwych, ograniczania mechanizmów uzależniających i większej transparentności działań tych platform adresowanych do dzieci. Skuteczna ochrona dzieci i młodzieży w środowisku cyfrowym wymaga równoczesnego działania na poziomie regulacji, egzekwowania prawa, edukacji, wsparcia rodziców, przygotowania szkół do właściwego reagowania i odpowiedzialności platform. W świetle ogromu i bezprecedensowego tempa rozwoju usług cyfrowych, a co za tym idzie zagrożeń, bezpieczeństwo dziecka online nie może być pozostawione wyłącznie jego własnej ostrożności – musi pozostać wspólną odpowiedzialnością dorosłych, instytucji publicznych i podmiotów kształtujących środowisko cyfrowe.

Źródło: NIK