

PROTOKÓŁ z V posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 27 października 2023 roku, o godzinie 13:00 w formie wideokonferencji.

Ochrona dzieci w Internecie- Pan Mikołaj Pawlak, Rzecznik Praw Dziecka oraz Pani Martyna Różycka z Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.

Pierwsza głos zabrała Pani Martyna Różycka z NASK przedstawiając charakterystykę Dyżurnet.pl, który został powołany w 2005 r. przez NASK. Zespół zajmuje się reagowaniem na treści internetowe przedstawiające seksualne wykorzystywanie osób małoletnich. Reaguje przede wszystkim na treści nielegalne, które są kierowane do Instytutu, jak również rozwija narzędzia, aby być krok przed przestępcami. Zastanawiając się nad bezpieczeństwem dzieci i młodzieży w Internecie należy wziąć pod uwagę, że inna jest sytuacja, gdy dziecko samo korzysta z Internetu i wymaga ochrony komunikując się z innymi użytkownikami, ale w przypadku treści przedstawiających seksualne wykorzystywanie osób małoletnich potrzeba ochrony również mówiąc o dziecku, jako ofierze (materiały są przekazywane między osobami postronnymi, natomiast prawa dziecka powinny być zachowane ze względu na to, że dziecko występuje na tego rodzaju materiałach). Od 2018 r. zadania Zespołu Dyżurnet.pl są wpisane jako zadania CSIRT NASK. Zespół jest częścią Safer Internet. W każdym europejskim kraju istnieje hotline – miejsce reagowania na nielegalne treści oraz helpline – miejsce, gdzie dzieci mają możliwość otrzymania pomocy psychologicznej. Prowadzone są również działania z zakresu propagowania bezpiecznego użytkowania Internetu. Zespół jest także członkiem międzynarodowego stowarzyszenia INHOPE. Zgłoszenia, które trafiają do Dyżurnet.pl dotyczą:

- materiałów przedstawiających seksualne wykorzystywanie dzieci,
- materiałów przedstawiających twardą pornografię,
- treści promujących rasizm i ksenofobię,
- innych nielegalnych treści, jak propagowanie lub pochwalanie zachowań o charakterze pedofilskim, uwodzenie dziecka poniżej 15 roku życia przez Internet, zjawiska szantażu na tle seksualnym.

Ostatnio Zespół miał także dużo zgłoszeń dotyczących Pandora Gate. Uznano, że potrzeba bardzo kompleksowego podejścia oraz dobrego rozumienia, w jaki sposób dzieci obecnie korzystają z Internetu.

Ponadto Pani Martyna Różycka wspomniała, że Zespół Dyżurnet.pl uczestniczy w pracach Zespołu do spraw przeciwdziałania przestępczości przeciwko wolności seksualnej i obyczajności na szkodę osób małoletnich powołanego przez Ministra Sprawiedliwości. Zespół miał na celu opracowanie Krajowego Planu Przeciwdziałania Przestępstwom Przeciwko Wolności Seksualnej i Obyczajności na Szkodę Małoletnich. Praca Zespołu oparta była o

międzynarodowy framework opracowany w ramach międzynarodowej organizacji WeProtect. Plan dotyczy kwestii, które powinny zostać podjęte na poziomie wymiaru sprawiedliwości, działań skierowanych do potencjalnych ofiar oraz do społeczeństwa. Istotne są procedury Notice and Takedown. Bardzo ważne, aby niewłaściwe treści zostały usunięte z Internetu, a także istotne jest przekazywanie zgłoszeń. Ważny jest także sposób, w jaki można wykorzystać technologię i czynniki, które pozwolą platformom blokować/nie publikować treści przedstawiających wykorzystywanie osób małoletnich, a także media, komunikacja oraz kwestie związane z samą świadomością zagrożeń.

Pan Mikołaj Pawlak, Rzecznik Praw Dziecka wskazał, że ochrona dzieci w Internecie może mieć wiele różnych aspektów. Weryfikowano z jakimi zjawiskami należy się zmagać, gdzie znajdują się problemy, jak wygląda struktura społeczności dzieci i młodzieży. W 2021 r. rozpoczęto ogólnopolskie badanie jakości życia dzieci w Polsce. Najszerze badanie od 2003 r. przeprowadzone zostało na dużej grupie dzieci i młodzieży ze wszystkich województw, regionów, z dużych i małych miast oraz ze wsi, z dużych szkół miejskich oraz małych szkół wiejskich. Do tej pory blisko 20 tys. dzieci i młodzieży zostało przebadanych. Każdy z badanych aspektów zawsze był oparty na podobnych kryteriach dla wykorzystania jako badanie naukowe. W 2021 r. w przerwie pandemii, gdy dzieci wróciły do szkół, było kilka aspektów przeprowadzonego badania dot. stosunku dzieci do szkoły, do rodziców, do ich zdrowia fizycznego/psychicznego, do relacji rówieśniczych. Badanie kontynuowano w 2022 r., a w 2023 r. będzie to badanie kompleksowe. Pan Rzecznik wskazał na stronę [Rzecznika Praw Dziecka](#). Jeden z kafelków to Ogólnopolskie badanie jakości życia dzieci i młodzieży w Polsce, gdzie przedstawione zostały wszystkie elementy i etapy przedmiotowego badania zawierające bardzo wiele aspektów życia młodych ludzi, ponadto podzielonych na grupy wiekowe, co jest istotne dla powtarzalności różnych zachowań i etapów życia. Są to pierwsze klasy szkół podstawowych, ostatnie klasy szkół podstawowych oraz szkoły ponadpodstawowe.

W kwietniu 2023 r. na posiedzeniu Rady ds. Młodzieży przy Narodowej Radzie Rozwoju zaprezentowany został Dziennik Codziennej Aktywności Dzieci i Młodzieży. Stworzono zakres czynności młodego człowieka od poranka przez przebieg dnia w szkole i poza szkołą do późnego wieczora. Jednym z bardzo istotnych aspektów tego badania była aktywność młodych ludzi w Internecie poprzez różnego rodzaju urządzenia. Pan Rzecznik przytoczył niektóre dane dotyczące czynności wykonywanych przez dzieci i młodzież, co jest zmienne w zależności od wieku młodych ludzi. Jednym z najbardziej zatrważających wyników przeprowadzonego badania było to, że 90% młodych ludzi niezależnie od wieku rano przed pójściem do szkoły ogląda filmiki na różnego rodzaju urządzeniach, a także używa social mediów co powoduje zagrożenia – behawioralne uzależnienia dzieci i młodzieży. Badanie z pewnością będzie dużym wkładem dla instytucji zajmujących się pedagogiką i wychowaniem dzieci. Kwestia ochrony dzieci w Internecie ma bardzo istotne znaczenie, ponieważ dorośli nie mają dostępu do ich świata. Nawet zakładając wiele różnego rodzaju ograniczeń młodzi ludzie zawsze znajdą dla nich obejście. Należy odpowiedzieć na pytanie, co dorośli mają do

przekazania w świecie dzieci i młodzieży, bo nie ma innej drogi, jak wejście w ich świat, a to oznacza wejście w świat Internetu i za pośrednictwem tego narzędzia przekazanie informacji młodym ludziom. Ponadto istotna jest kwestia wartości i autorytetów.

Pan Rzecznik zachęcił do zapoznania się z przytoczonymi badaniami, które są aktualne i zostały przeprowadzone na podstawie obiektywnych kryteriów stosowanych w całej Unii Europejskiej. W ostatnich latach zostało wprowadzonych wiele rozwiązań chroniących dzieci przed zagrożeniami w Internecie. Pan Rzecznik podsumowując wskazał, że Internet w ogromnej części uzależnia behawioralnie młodych ludzi, w skutek czego dzieci nie potrafią odbierać życiowych bodźców w prawidłowy sposób. Z pewnością będzie trzeba coraz bardziej zwracać uwagę na sposób, w jaki kształtujemy kolejne pokolenia. Empatia i wrażliwość kolejnych pokoleń przez bodźce z Internetu znacząco spada.

Pan Przewodniczący wskazał, że Rada powinna jak najszybciej zamknąć projekt stanowiska w przedmiotowym temacie. Uznał, że głębokim problemem jest to, iż rodzice i dzieci chcą mieć ze sobą relacje, jednak już nie potrafią. Pan Przewodniczący wskazał, że stanowisko Rady powinno być pogłębione o kontekst wychowawczy.

Jeden z członków Rady wspomniał o projekcie *Szkoła Gospodarki Cyfrowej Junior* dedykowanym dla VII i VIII klas, gdzie dzieci szkół podstawowych edukowane są z kompetencji cyfrowych. Ponadto pokazywana jest im także higiena korzystania z Internetu, ponieważ w szkole są braki, jeśli chodzi o tego typu edukację. Zauważono także niepokojące zjawisko, że coraz więcej dzieci jest hejtowanych w cyberprzestrzeni i z tego powodu doznają chorób psychicznych. Niepokojące jest, że niewielu rodziców korzysta z projektów edukacyjnych dla nich dedykowanych. Zatrważa również rosnące niebezpieczeństwo uzależnienia od Internetu i korzystanie z tego narzędzia do hejtowania. Stwierdzono, że rodzice muszą mieć świadomość prowadzenia dziecka również przez świat cyfrowy.

W toku dyskusji uznano, że problematykę budowania kompetencji cyfrowych od najmłodszych lat, ale również u rodziców należy zawrzeć w Krajowym planie działania do programu polityki „Droga ku cyfrowej dekadzie” do 2030 r.

Pan Rzecznik w dalszej wypowiedzi wspomniał także, iż od początku roku zanotowano dodatkowy wzrost połączeń na telefon zaufania wśród młodych ludzi.

Zauważone zostało, że być może kluczowa staje się wzajemna współpraca w przedmiotowym temacie i warto skupić inicjatywy prowadzone przez różne środowiska/organizacje działające na rzecz ochrony dzieci i młodzieży w tym obszarze.

Wspomniano o projekcie rozporządzenia o niegodziwym traktowaniu dzieci. Na konferencji prasowej w Parlamencie Europejskim grupa zajmująca się tym tematem poinformowała, że uzyskano tzw. porozumienie pomiędzy wszystkimi grupami politycznymi, co do głębokich zmian w propozycji Komisji Europejskiej. Głosowanie Parlamentu Europejskiego w tej sprawie zaplanowane jest na 13 listopada. Szereg kontrowersji, które zawiera projekt stanowiska ma szansę na usunięcie albo mocną redukcję.

Standardy Wspólnej Infrastruktury Informatycznej Państwa - Pan Jarosław Mojsiejuk oraz Pan Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa MC.

Pan Jarosław Mojsiejuk poinformował, że Rada otrzymała projekt *uchwały Rady Ministrów zmieniającej uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”*, co do której w pierwszej wersji było wiele różnych zastrzeżeń. Jedną z uwag Rady to powierzenie sektorowi publicznemu obowiązku dostarczania certyfikatów/oświadczeń, że dostawca ma spełniać standardy określone m.in. w Narodowych Standardach Cyberbezpieczeństwa. Podmiot publiczny zainteresowany korzystaniem z chmury publicznej czy też ze wszelkiego rodzaju chmur może mieć wątpliwość, który z narodowych standardów odpowiada standardom europejskim. W tle jest także punkt tzn. EUCS - standardy cyberbezpieczeństwa w chmurze. W obecnej wersji projektu został osiągnięty zasadniczy postęp. Zaiściały wątpliwości, czy można wprowadzić tzw. Samoistną uchwałę Rady Ministrów zakazy dotyczące możliwości przetwarzania w chmurze publicznej określonych rejestrów. Były także wątpliwości czy Minister Cyfryzacji powinien określać ważność rejestrów oraz co z tym może się wiązać. Uznano, że ostatni projekt uchwały zmierza w zdecydowanie dobrym kierunku.

Pan Dyrektor Marcin Wysocki na wstępie zauważył, że niektóre zmiany wynikające z nowelizacji projektowanej uchwały wprowadzają nowe rozwiązania, ale ich celem nie jest stworzenie dodatkowych obciążeń, ale zastąpienie tych, które obecnie wynikają z załącznika nr 2, zawierającego kryteria kwalifikacji systemów teleinformatycznych (mowa o obecnie obowiązującej *Uchwale nr 97 Rady Ministrów w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa"*¹ - kryteria klasyfikacji systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurach obliczeniowych) na bardziej adekwatne.

Rozpoczynając prace nad nowelizacją głównym asumptem do prac był fakt, iż załącznik nr 2 nie jest dostosowany do realiów i stanowi wyhamowanie rozwoju wykorzystania publicznej chmury obliczeniowej, którą można nazwać w języku potocznym bezpieczną chmurą komercyjną. Założeniem resortu cyfryzacji było usunięcie załącznika nr 2, a w zamian wprowadzenie zmian niektórych innych mechanizmów bezpieczeństwa, jak rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa w odniesieniu do gradacji systemów oraz katalog pewnych systemów teleinformatycznych, które w całości nie mogą być umieszczone w chmurze, co nie jest jednoznaczne z danymi w nich przetwarzanymi. Bardzo istotne i kluczowe jest to, iż uchwała Rady Ministrów może odnosić się i wiązać wyłącznie podmioty podległe Radzie Ministrów. W pozostałym zakresie w jakim dotyczy to innych podmiotów np. jednostek samorządu terytorialnego czy dostawców chmury obliczeniowej, resort podkreślał,

¹ Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa" (M.P. 2019 poz. 862).

że jest to dobrowolne, nie jest formalnie wiążące i postanowienia należy traktować jako rekomendacje, co jest wprost wskazane w nowym tekście.

Rozwiązania zawarte w uchwale są tak modyfikowane, aby uniknąć zarzutu, że uchwała kreuje obowiązki i uprawnienia niewynikające z prawa powszechnie obowiązującego. Wskazana jest możliwość korzystania z tego dobrodziejstwa uchwały przez podmioty nie mogące być nią związane w sposób formalny, ale które szukają eksperckiego wsparcia co do decyzji wykorzystania publicznej chmury obliczeniowej, dlatego wprost wskazano, że rekomendacje CSIRTu mają charakter fakultatywny. Mają one pomóc decydentom różnego szczebla podjąć decyzje o migracji rejestrów/ewidencji do chmury, które są oparte o dane przetwarzane w innych zasobach państwa. Pan Dyrektor odniósł się do kwestii mapowania, które jak uważa, można przeprowadzić wspólnie np. z grupą roboczą czy Radą. Pan Dyrektor zwrócił uwagę na to, iż intencją jest liberalizacja i w pewnym zakresie otworzenie się na rozwiązania chmurowe w administracji. Jeżeli obecnie obowiązujące rozwiązania nie są bardziej otwarte dla dostawców chmury publicznej, to oznaczałoby pewną porażkę tego projektu, ponieważ wszystkie rozwiązania zostały zaprojektowane jako otwierające nowe możliwości na wykorzystanie chmury komercyjnej. Jest jeszcze moment, aby kilka zmian/wątpliwości można było przeprosować. Pan Dyrektor wyjaśnił, że jeżeli posługujemy się pojęciem systemu teleinformatycznego to oznacza system, platformę, a nie dane w niej przetwarzane. I to różni definicje systemu teleinformatycznego i systemu informacyjnego. Odniesienie do definicji systemu teleinformatycznego powinno przeciąć dywagacje dotyczące możliwości przetwarzania danych wchodzących w skład rejestrów publicznych wskazanych w przepisach projektowanej uchwały w publicznej chmurze obliczeniowej.

Podziękowano za odpowiedzi Pana Dyrektora i zauważano, że pokrywają się z uwagami wskazanymi przez członków Rady. Wyraźnie podkreślono, że dokonano dużego postępu w aktualnej wersji projektu uchwały, zwłaszcza w zakresie popularyzacji usług chmury publicznej. Uznano, że można podjąć działania nad wspomnianym przez Pana Dyrektora mapowaniem. Wyrażono zadowolenie odnośnie prac nad dalszym rozwojem systemu ZUCH.

Pan Dyrektor wskazał, że w odniesieniu do uwag zgłoszonych przez RCL, resort zamierza wprowadzić kilka zmian - m.in. rezygnację z definicji podzielonej odpowiedzialności, jest możliwość przeprowadzenia mapowania w standardach cyberbezpieczeństwa chmury obliczeniowej, jest zależność ośrodków obliczeniowych oraz Centrum Przetwarzania Danych, od rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa dla tych podmiotów, które mogą być nimi objęte zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa.

[Dyskusja nad uwagami do projektu ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz ustawy – Kodeks postępowania administracyjnego.](#)

Zauważono, że temat jest szeroki - ustawa obejmuje także wspólną infrastrukturę informatyczną państwa, ponieważ dotyczy rejestrów państwowych oraz nowej koncepcji ram interoperacyjności, co do których różne instytucje zgłaszały mnóstwo uwag. W tle jest także

informacja o tsunami legislacyjnym UE – projekt *Digital Governance Act* oraz *Data Act*. Nie udało się uchwalić ustawy wprowadzającej DGA oraz innych aktów, które pozostają w związku z kluczową ustawą, tj. *ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne*. Celami ustawy jest m.in. optymalizacja działań administracji publicznej i wykorzystywanie nowoczesnych technologii w tym cloud computing. Zgłoszono uwagi dotyczące poszczególnych definicji, które znalazły się w projekcie diskutowanej ustawy. Pojawiły się wątpliwości co do definicji pojęcia rejestru publicznego, bowiem definicja zaproponowana w ustawie obejmowała praktycznie każdą bazę danych oraz definicji referencyjnego rejestru publicznego. Ponadto przepisy z zakresu podstawy do określenia architektury informacyjnej państwa robią wrażenie nieuporządkowanych. Uznano, że nowelizacja ustawy o informatyzacji jest potrzebna. Istotne jest wprowadzenie zasady domyślności cyfrowej. Potrzebna jest także nowelizacja uchwały o Wspólnej Infrastrukturze Informatycznej Państwa z budowaniem modelu wspólnej infrastruktury, podniesienie cyberbezpieczeństwa, odporności, rewitalizacji systemu ZUCH oraz nowelizacja Krajowych Ram Interoperacyjności, która powinna polegać m.in. na wskazaniu minimalnych wymagań w rozwoju ICT dla sektora publicznego oraz być może minimalnych wymagań w zakresie cyberhigieny.

W dalszej części zastanawiano się czy projekt *ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne* będzie podtrzymany w nowej kadencji Sejmu czy jednak będzie zmieniony, zatem formułowanie do niego uwag jest obecnie przedwczesne.

[Dyskusja nad finansowaniem i zwiększeniem kompetencji Ministerstwa Cyfryzacji.](#)

Zaproponowano przełożenie tematu na jedno z przyszłych spotkań Rady.

[Dyskusja nad powołaniem zespołów roboczych Rady \(w tym: NIS 2 i AI/SI\).](#)

Zaproponowano przełożenie tematu na jedno z przyszłych spotkań Rady.

[Standardy międzynarodowe kwalifikacji dot. Cyberbezpieczeństwa.](#)

Pan Jarosław Mojsiejuk wskazał, że wypełnia prośbę Polskiego Towarzystwa Informatycznego oraz Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo, która kieruje prośbę doprowadzenia, by kwalifikacje zdobywane i określone w Zintegrowanym Systemie Kwalifikacji mogły być także wykorzystywane do innych celów, ponieważ proces ich zdobywania jest oparty na programach/standardach, co najmniej tak samo wymagających jak standardy międzynarodowe określone w *Rozporządzeniu Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu*² zawierającym listę tych certyfikatów w rozumieniu ustawy o KSC. Zintegrowany System Kwalifikacji jest oparty o reguły i nadzorowany przez Ministra Cyfryzacji. Wśród 11 certyfikatów wymienionych w przytoczonym rozporządzeniu znajdują się same certyfikaty zagraniczne. Skierowano prośbę

² Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. 2018, poz. 1999).

o wystąpieniu Przewodniczącego Rady ds. Cyfryzacji do Ministra Cyfryzacji, aby certyfikaty uzyskiwane w ramach Zintegrowanego Systemu Kwalifikacji dopisać do listy zawartej we wskazanym rozporządzeniu.

Projekt uchwały Rady w sprawie problemu Dostawcy Wysokiego Ryzyka.

Pan Przewodniczący zarządził głosowanie nad uchwałą w elektronicznym trybie obiegowym.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Katarzyna Chałubińska-Jentkiewicz
3. Andrzej Dulka
4. Agnieszka Gryszczyńska
5. Agnieszka Jankowska
6. Jolanta Jaworska
7. Michał Kanownik
8. Janusz Kosiński
9. Dariusz Milka
10. Jarosław Mojsiejuk
11. Józef Orzeł - Przewodniczący
12. Marta Poślad
13. Tomasz Rychter
14. Krzysztof Silicki
15. Patrycja Staniszevska
16. Sławomir Wojciechowski

Zaproszeni goście:

17. Mikołaj Pawlak, Rzecznik Praw Dziecka
18. Martyna Różycka, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy
19. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczypospolitej Polskiej; Pełnomocnik Ministra Cyfryzacji do spraw relacji z podmiotami działającymi na rzecz rozwoju kompetencji cyfrowych
20. Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
21. Wiesław Paluszyński, ekspert Rady
22. Jacek Paziewski, ekspert Rady

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

23. Tomasz Opolski, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
24. Agnieszka Chruszcz, Naczelnik Wydziału, Departament Telekomunikacji w MC

25. Katarzyna Gójska, Biuro Ministra w MC
26. Olga Kunecka, Biuro Ministra w MC
27. Joanna Laskowska, Biuro Ministra w MC