PROTOKÓŁ z II posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 15 września 2023 roku, o godzinie 13:00 w formie wideokonferencji.

Omówienie wstępne projektów uchwał i stanowisk Rady:

Ochrona dzieci online;

Przedmiotowe stanowisko opiera się na dwóch projektach idących w tym samym kierunku tj. projektu ustawy o ochronie małoletnich przed dostępem do treści nieodpowiednich w Internecie oraz rozporządzenia Parlamentu Europejskiego i Rady ustanawiające przepisy mające na celu zapobieganie niegodziwemu traktowaniu dzieci w celach seksualnych i jego zwalczanie. Regulacja krajowa została wstrzymana ze względu na zbliżające się zakończenie obecnej kadencji Parlamentu RP. Wskazano pełną zgodę co do niezbędności przytoczonych aktów, potrzeb, kierunków wymienionych działań oraz szczególnie na zaangażowanie nie tylko sektora publicznego, ale także prywatnego w tym zakresie. Kwestią budzącą niepokój, która powinna wybrzmieć w stanowisku Rady, jest zmierzanie unijnego projektu zdecydowanie za daleko w kierunku ingerencji w prywatność osób i stanowienie o monitorowaniu chociażby korespondencji w poszukiwaniu ewentualnych zakazanych treści. Wspominany zapis zmierza zdecydowanie poza niezbędne działania w tym zakresie. Przede wszystkim narusza prywatność w nieodpuszczalny sposób zwłaszcza, że nawet przyjęty Digital Services Act, stanowi wprost, że nie można nakładać ogólnego obowiązku monitorowania informacji, które dostawcy usług przekazują/przechowują ani aktywnego ustalania faktów lub okoliczności wskazujących na nielegalną działalność. Ten aspekt był także wielokrotnie podnoszony przez polski rząd, a także przez branżę cyfrową oraz wiele krajów członkowskich co do narzędzia, które wprowadza regulacja europejska mówiąca o monitorowaniu/ingerowaniu w prywatność osób w żaden sposób nie uwikłanych w jakiekolwiek postępowanie w tej materii. Podkreślone zostało, że stanowisko Rady apeluje tylko i wyłącznie o przemyślenie przedmiotowej kwestii. Co do zasady i kierunku działania jest pełna aprobata Rady dla regulacji unijnych oraz celu, który temu przyświeca.

DWR;

Zaproponowany projekt uchwały jest kontynuacją prac poprzedniej kadencji Rady. Nowe fakty, które mogą mieć istotne znaczenie dla tej problematyki to przede wszystkim stanowisko Komisji Europejskiej, które pojawiło się po drugim przeglądzie Toolbox 5G, czyli zestawu narzędzi, którymi państwa mogą operować w celu zapewnienia bezpieczeństwa czy cyberbezpieczeństwa sieci telekomunikacyjnych piątej generacji. Wspomniano o dokonanym przeglądzie i sporządzonym raporcie, w wyniku którego w oświadczeniach Komisji Europejskiej pojawiły się zdecydowane stwierdzenia, że istnieją podstawy do uznania wskazanych chińskich dostawców za DWR. W konsekwencji Komisja Europejska zakazała zamawiania produktów telekomunikacyjnych tych firm na własne potrzeby, tj. dla samej Komisji i jej agend czy przedstawicielstw itp. Projekt uchwały Rady powstał, kiedy istniała szansa, że skierowany do parlamentu przez rząd projekt ustawy o krajowym systemie cyberbezpieczeństwa, wprowadzający do polskiego porządku prawnego instytucję DWR,

znajdzie się w polskim ustawodawstwie ze wszelkimi konsekwencjami. Projekt ww. ustawy został przez rząd wycofany ze względu na dyskontynuację. Wskazano, że projekt uchwały Rady częściowo będzie wymagał lekkiej korekty, ale stanowi kontynuację myśli, które były zawarte w poprzednich stanowiskach Rady.

Jeden z członków Rady zaznaczył, że projekt uchwały jest szerszy. Temat DWR nie odnosi się tylko do ustawy o krajowym systemie cyberbezpieczeństwa (KSC) i budowy sieci 5G. DWR jest to wyzwanie generalne dla polskiego i europejskiego rynku. Mając na uwadze, że nowelizacja ustawy o KSC nie weszła w życie, niezbędne jest stworzenie jak najwięcej jasnych stanowisk ze strony instytucji państwa w kontekście definicji pojęcia DWR oraz sposobu uniknięcia używania jego technologii szczególnie w infrastrukturze krytycznej. Istotne jest, by przekaz ekspercki ze strony Rady trafił do maksymalnie szerokiego grona odbiorców instytucjonalnych w Polsce.

Wyrażono przekonanie, że Rada powinna wspierać przedmiotowy temat jako bardzo istotny. Podkreślone zostały kwestie bezpieczeństwa i obronności oraz pewne działania po stronie NATO, które zmierzają do zwiększenia odporności systemowej państwa, gdzie sieci telekomunikacyjne są wymienione jako jeden z priorytetów. Wydaje się, że aktualna dynamika geopolityczna narzuca oczywiste wnioski z tym związane w obszarze DWR. Zaproponowano uaktualnienie stanowiska Rady po wyborach parlamentarnych o dodatkowe informacje/argumenty, jakie mogłyby wynikać z dynamiki politycznej po stronie Unii Europejskiej czy innych instytucji, a także przykładów z innych krajów, które podjęły w tym kierunku pewne kroki.

W toku dyskusji wyrażono zdanie, że im więcej opinii eksperckich w tym zakresie, tym będzie łatwiej wielu instytucjom, również tym, które np. będą zainteresowane sieciami prywatnymi - dużym biznesom czy samorządom, podjąć decyzje, skoro nie ma odniesienia ustawowego w KSC.

Pan Przewodniczący wskazał, że Rada powinna jasno powiedzieć w stanowisku, iż w części przetargów stosowanie kryterium ceny albo dużej dominacji wskaźnika ceny powoduje, że dostawcy tacy jak chińscy, są preferowani. Względy bezpieczeństwa powinny odgrywać bardzo dużą rolę. Należy wskazać działania, jakie podejmują w tej sprawie poszczególne kraje, Komisja Europejska i NATO.

Jeden z członków Rady wskazał, że w kontekście DWR nie chodzi o konkretną technologię czy generację sieci takiej jak 5G, lecz o pewną kategorię zagrożenia ze strony producentów czy dostawców. Zaproponowano dodanie do projektu uchwały zapisu mówiącego o bezpieczeństwie łańcucha wartości. Istotne jest, aby te zasady działały w przypadku zakupu sprzętu, oprogramowania czy usług.

W toku dyskusji pojawiła się propozycja, by powstały rekomendacje Prezesa UZP choćby w zakresie wymagań technicznych, które będą do zastosowania dla jednostek publicznych w zakresie cyberbezpieczeństwa, DWR czy też łańcucha dostaw. Bez opublikowania przez Prezesa UZP jasnych wytycznych czy zaleceń nie uda się pokonać aspektu ceny, który będzie

wygrywał w znacznej części przypadków. Ponadto wskazane zostało, że projekt uchwały czy dyskusja o DWR nie odnoszą się tylko do interesu firm, lecz do bezpieczeństwa narodowego, ale też, że instytucja DWR nie może dotyczyć tylko telekomunikacji, ale także innych sfer.

Uznano, że projekt stanowiska o DWR należy wzbogacić o kwestie związane z kryteriami przetargów w PZP.

Zakup laptopów do szkół;

Zaproponowano powstanie stanowiska Rady w kontekście zakupu laptopów do szkół i powiązanego z tym zmodernizowania pracowni komputerowych dla zabezpieczenia przed incydentami, przygotowania szkół pod kątem sieci elektrycznych, a także sposobu wykorzystania komputerów w pracy dydaktycznej. Zaproponowano także, aby na jednym z posiedzeń Rady podjąć dyskusję na temat wykonania dostaw laptopów a zadań w tym zakresie samorządów i szkół.

Grupy robocze MC;

Pani Dyrektor Inez Okulska wspomniała, że Departament Innowacji i Technologii MC jest we współpracy z grupami roboczymi oraz o przeprowadzeniu reorganizacji grup. Wynika to z faktu zgromadzenia grona ponad 700 ekspertów w dziedzinie m.in. sztucznej inteligencji. W planach jest wiele działalności we współpracy z tymi ekspertami.

Ewakuacja danych IK do chmury;

Jeden z członków Rady przedstawił wstępny projekt uchwały o podniesieniu poziomu odporności ewakuacji do chmury. Istotą jest, aby każdy podmiot, który jest podmiotem infrastruktury krytycznej, w szerszym kontekście - prac nad Dyrektywą NIS2, przygotował plan ewakuacji do chmury obliczeniowej. W przedmiotowym projekcie uchwały znajduje się także postulat powołania zespołu w celu wymiany doświadczeń z Ukrainą, gdzie Polska mogłaby pełnić rolę koordynacyjną w szczególności w państwach Trójmorza. Zasugerowano włączenie do niej nowych członków NATO (Szwecję i Finlandię) i ujednolicania tego typu procedur. W projekcie uchwały zawarto też przypomnienie o przygotowaniu planu dotyczącego e-Ambasady.

Pani Dyrektor Joanna Baranowska odniosła się do tematu e-Ambasady. Wizja projektu została zatwierdzona. Trwają przygotowania koncepcji realizacji oraz przygotowanie wniosku o dofinansowanie. Prace w tej materii są bardzo intensywnie prowadzone.

Wstępna dyskusja nad tematami i materiałami zgłoszonymi przez członków Rady:

Dostęp lekarzy do danych pacjentów.

Jeden z członków Rady zaproponował dyskusję na temat problemu wypracowania rekomendacji w zakresie polityki bezpieczeństwa informacji dla systemów informatycznych. Wspominano o incydencie dotyczącym systemu e-pacjent, który wpisuje się w kanon cyberbezpieczeństwa. Zauważono, że w jednostkach samorządu do realizacji zadań własnych zastosowanych jest kilkadziesiąt systemów informatycznych najczęściej wywodzących się od

dostawców komercyjnych, biorąc pod uwagę wielką ilość przetwarzanych informacji o zróżnicowanym stopniu znaczenia i krytyczności tj. dane osobowe czy finansowe. Pytanie - czy na etapie projektowania różnego rodzaju rozwiązań informatycznych uwzględnia się bezpieczeństwo informacji. Najczęściej uwaga skupia się na tym, aby system był ergonomiczny i przyjazny dla użytkownika. Zaproponowano, aby przedmiotową kwestię przedyskutować w ramach Rady i zwrócić się do Ministerstwa Cyfryzacji o wsparcie kompetencyjne.

W toku dyskusji zauważono, że dostęp do danych medycznych przez kadrę medyczną za zgodą pacjenta wynika z przepisów. Wyjątkiem jest np. sytuacja ratowania życia. Zgoda pacjenta udzielana jest najłatwiej na Internetowym Koncie Pacjenta. Wracając do incydentu związanego z systemem e-pacjent konieczna jest zmiana przepisów, a przez to także architektury systemu P1, ponieważ poziom cyfryzacji w ochronie zdrowia jest dużo większy, a w związku z tym potrzebna jest ustawa o dokumentacji medycznej. Obecnie trwają zaawansowane prace nad przepisami unijnymi, wprowadzającymi wymianę danych medycznych na poziomie unijnym, gdzie zaprojektowane zostały przepisy dotyczące dostępu do danych, które także wpłyną na kształt regulacji w Polsce. Przytoczony incydent doprowadził do braku zaufania obywateli w zakresie bezpieczeństwa danych w różnego rodzaju rejestrach centralnych. W e-zdrowiu dane mogą ratować zdrowie i życie. Należy więc odwrócić ten trend i uświadomić społeczeństwu, że dane z zakresu zdrowia są bezpieczne.

Pan Przewodniczący zaproponował stworzenie zespołu redakcyjnego w tematyce sposobu zabezpieczenia systemów teleinformatycznych w medycynie. Pan Przewodniczący zaproponował dodanie do tematu medycznego następujących kwestii:

- Status własności i dysponowania danymi medycznymi.
- Rola edukacyjna dot. danych medycznych.
- Czy potrzebne są standardy bezpieczeństwa czy wystarcza sama edukacja dotycząca zbierania danych przez zagraniczne koncerny przy użyciu aplikacji i wyrobów medycznych, takich jak smartwatche, opaski i inne urządzenia codziennego użytku, które zbierają dane?

Pan Przewodniczący zaproponował, aby Rada podjęła temat finansowania i zwiększenia kompetencji Ministerstwa Cyfryzacji. Poprosił też członków Rady o uwagi do wszystkich projektów oraz tematów, także do tych, które jeszcze nie były omawiane.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Agnieszka Gryszczyńska
3. Agnieszka Jankowska
4. Michał Kanownik
5. Agnieszka Kister
6. Janusz Kosiński
7. Anna Beata Kwiatkowska
8. Dariusz Milka
9. Jarosław Mojsiejuk
10. Józef Orzeł - Przewodniczący
11. Marta Poślad
12. Tomasz Rychter
13. Krzysztof Silicki
14. Robert Trętowski
15. Sławomir Wojciechowski
16. Małgorzata Zakrzewska

Zaproszeni goście:

17. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczpospolitej Polskiej; Pełnomocnik Ministra Cyfryzacji do spraw relacji z podmiotami działającymi na rzecz rozwoju kompetencji cyfrowych
18. Joanna Baranowska, Dyrektor Departamentu Wspólnej Infrastruktury Informatycznej Państwa w Centralnym Ośrodku Informatyki
19. Mariusz Truss, Architekt do spraw sieci w Centralnym Ośrodku Informatyki
20. Wiesław Paluszyński, ekspert Rady
21. Jacek Paziewski, ekspert Rady
22. Przemysław Sypniewski, ekspert Rady

Sekretariat Rady i pracownicy Ministerstwa Cyfryzacji:

23. Marzena Sawicka, Zastępująca Dyrektora Generalnego, Dyrektor Departamentu Telekomunikacji w MC

24. Inez Okulska, Dyrektor Departamentu Innowacji i Technologii w MC
25. Tomasz Opolski, Zastępca Dyrektora Departamentu Telekomunikacji w MC
26. Michał Pukaluk, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa w MC
27. Agnieszka Chruszcz, Naczelnik Wydziału, Departament Telekomunikacji w MC
28. Łukasz Różycki, Starszy specjalista, Departament Telekomunikacji w MC
29. Alan Kosecki, Administrator, Departament Cyberbezpieczeństwa w MC
30. Mateusz Karaś, Radca, Departament Cyberbezpieczeństwa w MC
31. Katarzyna Stopińska, Biuro Ministra w MC
32. Katarzyna Gójska, Biuro Ministra w MC
33. Olga Kunecka, Biuro Ministra w MC