

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

- **KOMISJI CYFRYZACJI, INNOWACYJNOŚCI
I NOWOCZESNYCH TECHNOLOGII
(NR 51)
z dnia 20 maja 2025 r.**

Pełny zapis przebiegu posiedzenia Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 51)

20 maja 2025 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Bartłomieja Pejo (Konfederacja)**, przewodniczącego Komisji, zrealizowała następujący porządek dzienny:

– rozpatrzenie informacji na temat stanu prac nad implementacją przepisów NIS2 i 5G Toolbox.

W posiedzeniu udział wzięli: **Marcin Wysocki** zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji, **Marcin Brzeziński** ekspert w Departamencie Bezpieczeństwa Urzędu Komunikacji Elektronicznej, **Grzegorz Gontarz** radca prawny w Wydziale Prawno-Legislacyjnym w Biurze Rzecznika Małych i Średnich Przedsiębiorców, **Michał Kanownik** prezes Zarządu Związku Cyfrowa Polska, **Grzegorz Lang** dyrektor ds. prawnych w Federacji Przedsiębiorców Polskich, **Justyna Wilczyńska-Baraniak** liderka zespołu oraz Szymon Skalski prawnik w Zespole Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska wraz ze współpracownikami, **Tomasz Bukowski** ekspert ds. telekomunikacji Polskiej Izby Komunikacji Elektronicznej, **Piotr Radecki** ekspert Konfederacji Lewiatan, **Krzysztof Komorowski** ekspert Polskiego Towarzystwa Informatycznego, **Michał Smagowicz** wiceprezes, członek Zarządu THINKTANK, **Daniela Werbeniec** dyrektorka Forum Cyfrowego Związku Przedsiębiorców i Pracodawców, **Klaudia Bazyk** menadżer ds. projektów Polskiej Izby Handlu, **Sonia Kurpiel** specjalista do spraw legislacji w Polskim Towarzystwie Gospodarczym, **Joanna Karczewska** przedstawicielka Stowarzyszenia Absolwentów Elektroniki na Politechnice Warszawskiej @ELKAPW oraz **prof. ucz. dr hab. Marta Grabowska** wykładowca w Centrum Europejskim Uniwersytetu Warszawskiego.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Leszek Jasiński** i **Magdalena Krzymowska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dzień dobry państwu. Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

Stwierdzam kworum.

Witam panie i panów posłów. Witam przedstawiciela Ministerstwa Cyfryzacji pana Marcina Wysockiego, zastępcę dyrektora Departamentu Cyberbezpieczeństwa. Witam reprezentantów strony społecznej, urzędów, instytucji: Urzędu Komunikacji Elektronicznej, Biura Rzecznika Małych i Średnich Przedsiębiorców, przedstawiciela Ernst&Young, Konfederacji Lewiatan, Związku Cyfrowa Polska, Polskiej Izby Komunikacji Elektronicznej, THINKTANK, Związku Przedsiębiorców i Pracodawców, Polskiej Izby Handlu, Polskiego Towarzystwa Gospodarczego, Stowarzyszenia @ELKAPW, a także Centrum Europejskiego Uniwersytetu Warszawskiego. Witam wszystkich państwa bardzo serdecznie.

Drodzy państwo, porządek dzisiejszego posiedzenia przewiduje rozpatrzenie informacji ministra cyfryzacji na temat stanu prac nad implementacją przepisów NIS2 i 5G Toolbox.

Czy są uwagi do dzisiejszego porządku obrad? Nie widzę, zatem przechodzimy do realizacji punktu, który przedstawi pan dyrektor Wysocki. Proszę o ustne zreferowanie stanu prac nad implementacją NIS 2 i 5G Toolbox. W dyskusji będę chciał też przekazać głos pani Justynie Wilczyńskiej-Baraniak, która zreferuje raport na temat tego punktu.

Oddaję głos panu dyrektorowi Wysockiemu. Bardzo proszę, panie dyrektorze, o zreferowanie tego punktu.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji Marcin Wysocki:

Bardzo dziękuję. Panie przewodniczący, Wysoka Komisjo, szanowni państwo, projekt ustawy o zmianie ustawy o krajowym systemie bezpieczeństwa oraz niektórych ustaw wdraża dyrektywę Parlamentu Europejskiego z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii tzw. dyrektywy NIS2, której termin transpozycji upłynął 17 października 2024 r. Pojawienie się nowych cyberzagrożeń, szybki wzrost katalogu usług publicznych dostępnych online powodują, że instytucje publiczne, jak i podmioty prywatne odpowiedzialne za cyberbezpieczeństwo będą zmuszone poświęcać coraz więcej środków na jego zapewnienie. Zmieniająca się sytuacja międzynarodowa oraz konieczność dostarczania usług dużej grupie nowych klientów sprawia, że niezbędne jest dalsze wzmacnianie podmiotów krajowego systemu cyberbezpieczeństwa.

Wdrożenie dyrektywy NIS2 na poziomie krajowym zwiększy poziom cyberbezpieczeństwa w kraju, w Unii Europejskiej, w szczególności poprzez zbudowanie zdolności w zakresie cyberbezpieczeństwa, łagodzenie zagrożeń dla sieci systemów informatycznych wykorzystywanych do celu świadczenia usług kluczowych oraz zapewnienia ciągłości działania.

Podsumowując etapy procesu legislacyjnego, projekt ustawy o zmianie ustawy o KSC został wpisany do wykazu prac legislacyjnych i programowych Rady Ministrów 8 kwietnia 2024 r. Do konsultacji publicznych projekt skierowano 24 kwietnia 2024 r. W ramach procesu konsultacji publicznych uwagi zgłosiło 96 podmiotów. Szereg uwag zgłosili członkowie Rady Ministrów oraz inne organy centralne. Z powodu znacznej liczby uwag – a tabele uwag łącznie mają ponad tysiąc stron – prace nad ich rozpatrzeniem i przygotowanie nowej wersji projektu trwały do początku października 2024 r. 14 stycznia już bieżącego roku projekt uzyskał pozytywną wiążącą opinię Komisji Wspólnej Rządu i Samorządu Terytorialnego. Został do tego upoważniony Zespół do Spraw Społeczeństwa Informacyjnego. Projekt został skierowany do rozpatrzenia przez Komitet do Spraw Europejskich. KSE przyjął projekt po potwierdzeniu w dniu 13 lutego oraz rekomendował rozpatrzenie projektu ustawy wraz z protokołem rozbieżności Stałemu Komitetowi Rady Ministrów. W dniu dzisiejszym Komitet Rady Ministrów do spraw Bezpieczeństwa Narodowego również pozytywnie zaopiniował projekt. Więc albo już, albo za chwilę taka komunikacja zostanie przekazana na Stały Komitet Rady Ministrów. Natomiast 27 listopada Komisja Europejska wystosowała w trybie art. 258 Traktatu o funkcjonowaniu Unii Europejskiej zarzuty formalne dotyczące braku wdrożenia dyrektywy NIS2. 5 lutego przekazaliśmy odpowiedź na zarzuty formalne Komisji Europejskiej, w którym wskazyaliśmy, że prace parlamentarne nad projektem przypadną na pierwszą połowę bieżącego roku. Odpowiedź została wcześniej uzgodniona w ramach Komitetu do Spraw Europejskich. Komisja Europejska skierowała wobec Polski tzw. uzasadnioną opinię w związku z niewdrożeniem dyrektywy NIS2 w terminie.

Odpowiedź oczywiście zostanie przygotowana przez ministra cyfryzacji, uzgodniona z Komitetem do Spraw Europejskich oraz przekazana do Komisji Europejskiej do 7 lipca 2025 roku, bo taki termin wynika z tego pisma Komisji.

Co jest również istotne, jestem przekonany, że ministra cyfryzacji i całego rządu nie trzeba dodatkowo motywować, ale oczywiście przyjęcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest również kamieniem milowym bardzo ważnej reformy C3.1.1. Krajowego Planu Odbudowy i Zwiększania Odporności. Z tych i oczywiście z wielu jeszcze innych powodów projekt ma charakter pilny i priorytetowy.

Jeżeli chodzi o takie kluczowe, związane zagadnienia, które obejmuje projekt, są one wskazane w materiale do Komisji. Dziękuję, panie przewodniczący.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję, panie dyrektorze. Motywować może nie trzeba, natomiast widzimy, że te terminy mijają – jeden, drugi, trzeci i stąd też pytanie. Strona społeczna i parlamentarzyści chcieli wiedzieć i chcą wiedzieć, jak wygląda bieżąca praca nad tym projektem. Stąd też dzisiaj Komisja w tej sprawie.

Proszę państwa, czy ktoś z pań i panów posłów chciałby zabrać głos w tym punkcie? Nie widzę. Jest? Pan poseł? Bardzo proszę, poseł Bliźniuk.

Posel Paweł Bliźniuk (KO):

Tak. Mam jedno bardzo krótkie pytanie. Takie pytanie, ale też prośba o jakieś zobowiązanie. Kiedy finalnie możemy spodziewać się tego projektu?

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Panie pośle, projekt jak najszybciej stanie na Stałym Komitecie Rady Ministrów. Potem kolejnym takim dużym i istotnym etapem jest przyjęcie projektu przez Radę Ministrów. Oczywiście wg. potrzeb może zostać również przeprowadzona komisja prawnicza.

Czujemy to zobowiązanie i chcemy, żeby projekt jak najszybciej trafił do prac parlamentarnych. W Komisji, w tym zobowiązaniu wskazaliśmy, że projekt zostanie przekazany do parlamentu jeszcze w bieżącym półroczu.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Pan poseł Bliźniuk.

Posel Paweł Bliźniuk (KO):

Został ponad miesiąc.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Właśnie, pozostał ponad miesiąc.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Panie przewodniczący, jestem przekonany co do tego, że poza planowanymi posiedzeniami Rady Ministrów posiedzenia w ważnych tematach są też zwoływane ad hoc. Mamy takie poczucie, że wszyscy czujemy gravitas z jednej strony do zapewnienia cyberbezpieczeństwa, tam są niezbędne środki.

Jeżeli chodzi o środki ze strony państwa do podjęcia adekwatnych działań w cyberprzestrzeni, to co chciałbym powiedzieć, jeżeli chodzi o tę ustawę, to zawiera ona dwa komponenty: wdrożenie dyrektywy NIS2 i Toolbox 5G.

Jeżeli chodzi o wdrożenie dyrektywy NIS2, to jesteśmy w zaszczytnym gronie 19 państw europejskich, które nie wdrożyły transpozycji w terminie. Przypomnę, że termin transpozycji minął w październiku poprzedniego roku.

Natomiast we wdrożeniu Toolbox 5G niestety jesteśmy na samym końcu, bo już zdecydowane dwadzieścia kilka państw oświadczyło, że wdrożyło Toolbox 5G. Część z tych państw również już podjęło środki stosowania prawa, konkretne ograniczenia związane z Toolbox 5G. W tej statystyce niestety jesteśmy na niechlubnym końcu lub jednym z ostatnich kilku państw.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję za to przekazanie informacji. Nie nazwałbym może zaszczytnym tego grona, które pan dyrektor wymienił. Chyba wszyscy widzimy, że jest potrzeba jak najszybszego procedowania w tym zakresie.

Czy ktoś z pań i panów posłów jeszcze chciałby zabrać głos?

W takim razie otwieram dyskusję również w sferze strony społecznej. Bardzo proszę o zgłoszenia. Czy ktoś z państw chciałby zabrać głos w tym zakresie? Bardzo proszę. Pan prezes Kanownik, bardzo proszę.

Prezes Zarządu Związku Cyfrowa Polska Michał Kanownik:

Dziękuję, bardzo.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dla formalności proszę się oczywiście przedstawiać.

Prezes Zarządu Związku Cyfrowa Polska Michał Kanownik:

Michał Kanownik, prezes Zarządu Związku Cyfrowa Polska.

Panie przewodniczący, dziękuję za głos. Panie dyrektorze, dziękujemy za tę informację. Ona nie jest pewnie tak zadowalająca, jak wszyscy byśmy chcieli, bo już wszyscy byśmy chcieli, żeby projekt był wreszcie uchwalony w Sejmie, bo jest po czasie.

Natomiast chciałem podkreślić znaczenie tego projektu właśnie od strony biznesu, nie tylko ze względu na mijające terminy transpozycji NIS2 czy też Toolbox jako jedni z ostatnich, ale mówimy o bardzo kluczowych aspektach funkcjonowania na rynku. Nie chodzi tylko o bezpieczeństwo infrastruktury państwowej, ale przede wszystkim o bezpieczeństwo

funkcjonowania biznesu generalnie w Polsce. I ta ustawa jest niezmiernie wyczekiwana i ważna. Wszyscy trzymamy kciuki, żeby udało się dotrzymać tych terminów, o których pan dyrektor wspomniał, bo jest to, śmiem twierdzić, najdłużej konsultowany projekt ustawy w historii polskiego parlamentaryzmu. Żadna ustawa nie była tak długo dyskutowana, konsultowana, uzgadniana jak ta, więc może – trzymam za to kciuki – przynajmniej dzięki temu bardzo sprawnie przejdzie ona przez parlament, już bez nadmiernych dyskusji.

Chciałem podkreślić tylko jedną rzecz, że ze strony biznesu jest pełne zrozumienie tego, że kiedy mówimy o kwestiach bezpieczeństwa, to nie wolno tego przekładać na kwestie oszczędności. Znaczący na bezpieczeństwie nie wolno oszczędzać, i to, mam nadzieję, że będzie się przewijało w pracach nad tą ustawą i będzie podtrzymane to podejście, że mówimy o inwestycjach, które są niezbędne dla ciągłości funkcjonowania i państwa i biznesu w Polsce.

Tu nie ma miejsca na kompromisy, dlatego liczymy i trzymamy kciuki za to, żeby ta ustawa trafiła do Sejmu, była sprawnie procedowana i weszła w życie, bo to jeszcze raz podkreślę, jest w interesie nas wszystkich. Biznes trzyma kciuki absolutnie z całej mocy i będziemy starali się wspierać rząd w tym zakresie, żeby ta ustawa jak najszybciej została przyjęta przez parlament. Dziękuję.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję. Pan poseł Bliźniuk?

Poseł Paweł Bliźniuk (KO):

Tak, ja chciałem podziękować za ten głos mojego przedmówcy, ale stanę w obronie długotrwałej, kwiecistej historii polskiego parlamentaryzmu. Otóż chciałem nadmienić, że nie ma jeszcze projektu ustawy, więc my nie mamy czym się zajmować. Żeby nie pozostało takie wrażenie, że...

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Mobilizujemy.

Poseł Paweł Bliźniuk (KO):

To nie parlament tutaj jest tym czynnikiem, który powoduje zwłokę. My mobilizujemy stąd też to posiedzenie i rozmowa na ten temat. Myślę, że komisja cyfryzacji to miejsce, gdzie pracujemy ponad podziałami politycznymi i czekamy na ten projekt, bo wiemy, jak ważny jest dla biznesu, jak ważny jest dla naszego bezpieczeństwa.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję i popieram w pełni wypowiedź mojego poprzednika.

Bardzo proszę, przekazuję głos dalej.

Prawnik w Zespole Własności Intelektualnej, Technologii i Ochrony Danych Osobowych w EY Polska Szymon Skalski:

Dzień dobry państwu, Szymon Skalski EY Poland.

Mam takie pytanie do pana dyrektora, odnośnie do tych dwóch poprzednich pytań, pojawia się takie pytanie też ze strony biznesu. Z tego co widać w mediach, tych kwestii poruszanych..., bo oprócz NIS2 na poziomie Unii Europejskiej została też przyjęta ta dyrektywa CER, która znajduje się dość niedaleko w dzienniku unijnym i ona też musi być implementowana. Tak naprawdę ona jest mocno powiązana terminologicznie, prawnie z NIS2.

I teraz jest pytanie czy tak naprawdę mamy spodziewać się kolejnego projektu UKSC harmonizującego UKSC z tym, co będzie wdrażało dyrektywę CER. Tak naprawdę to jest pytanie, czy po prostu będziemy teraz mieli szósty projekt tej ustawy, czy piąty to jest to, co będziemy mieli.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję. Proszę o odpowiedź, panie dyrektorze.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Panie przewodniczący, to już może rozbije ten wazon – na każdy etap procesu legislacyjnego powstaje nowa wersja. Więc mogę powiedzieć, że będzie szósta, siódma, ósma w parlamencie.

Natomiast już odnosząc się merytorycznie do tego zagadnienia, gospodarzem tego drugiego projektu ustawy wdrażającej dyrektywę CER, czyli o zmianie ustawy o zarządzaniu kryzysowym, ściśle współpracujemy z zespołem Rządowego Centrum Bezpieczeństwa.

Pracujemy nad tym, żeby ta linia demarkacyjna co do obowiązków była jasno wytyczona, żeby absolutnie ten nadzór się na siebie nie nakładał, żeby te wszystkie kwestie otoczenia regulacyjnego oddzielić, żeby te obowiązki były jak najbardziej adekwatne, przemyślane, bo zdajemy sobie sprawę, że tych podmiotów, które będą objęte, co wynika z logiki tych aktów prawnych podmiotów kluczowych, podmiotów krytycznych, będzie naprawdę bardzo dużo, więc chcemy zadbać o to, żeby te przepisy były jak najbardziej spójne ze sobą, co znacznie ułatwi ich wdrażanie, a przede wszystkim osiągnięcie celu, czyli zwiększenie odporności w tym wymiarze fizycznym i cyberbezpieczeństwa.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję i proszę.

Ekspert ds. telekomunikacji Polskiej Izby Komunikacji Elektronicznej Tomasz Bukowski:

Dziękuję, panie przewodniczący. Tomasz Bukowski, ekspert Polskiej Izby Komunikacji Elektronicznej.

Nasza Izba, oczywiście też razem z innymi izbami telekomunikacyjnymi, przygląda się temu projektowi ustawy. Jak najbardziej potwierdzamy, że kwestie bezpieczeństwa, cyberbezpieczeństwa są bardzo istotne. Niemniej jednak po raz kolejny chcemy wskazać, że problemy z całym projektem ustawy i to, dlaczego ona jest tak długo procedowana, nie wynikają z implementacji NIS2 czy Toolbox 5G, ale z wyjścia poza te dwie regulacje unijne, znacznego wyjścia.

I o ile naszym priorytetem jako przedsiębiorcy funkcjonującego w Polsce oczywiście jest kwestia bezpieczeństwa, to również jest to kwestia bezpieczeństwa gospodarczego naszych podmiotów. Mamy poważne obawy związane z tak szerokim i mocnym wyjściem, naszym zdaniem wykraczającym poza cele tych regulacji unijnych i nawet poza cele deklarowane przez ministerstwo o nieokreślonych, a potencjalnie bardzo trudnych skutkach gospodarczych tej ustawy. Dziękuję bardzo.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo. Czy pan dyrektor może się odnieść do tego stwierdzenia?

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Oczywiście, panie przewodniczący. Jak minister finansów ogląda każdą złotówkę budżetu, tak wszystko, co wychodzi poza minimalny poziom harmonizacji, czyli tę zasadę wynikającą z wdrożenia dyrektywy, minister cyfryzacji z partnerami, z innymi ministrami ogląda trzykrotnie, czy jest to szczególnie uzasadnione, żeby wprowadzić takie daleko idące rozwiązanie.

Zawsze jestem otwarty na dyskusję o poszczególnych rozwiązaniach. Natomiast niestety w przestrzeni publicznej gold-platingiem określa się wiele rozwiązań, które wprost wynikają z dyrektywy NIS2. I to niestety troszeczkę nam przekształca i utrudnia debatę publiczną, ponieważ to, co jest dalej idącym środkiem, to, co nie wynika z dyrektywy NIS2, to, co projektodawca dodał z jakichś uzasadnionych przyczyn, to możemy nazywać nadregulacją i o tym możemy dyskutować. Rozumiem tutaj przedstawicieli biznesu, że zgłaszają do tego uwagi, natomiast wiele z tych rzeczy wynika wprost z dyrektywy NIS2. I na to wyczulam.

Jeżeli jest jakieś bardziej szczegółowe pytanie, to oczywiście jestem do dyspozycji.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo. Czy ktoś jeszcze z państwa chciałby zabrać głos?

Pani Justyno, czy teraz możemy? W takim razie bardzo proszę, pani Justyna Wilczyńska-Baraniak, która, jak rozumiem, przedstawi raport na ten temat. Bardzo proszę.

Liderka zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska Justyna Wilczyńska-Baraniak:

Bardzo dziękuję. Szanowna Komisjo, drodzy państwo, dziękuję za możliwość przedstawienia wniosków z raportu. Jako adwokat i lider zespołu prawnego do spraw cyberbezpieczeństwa w regionie EMEA...

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Przepraszam, troszeczkę bliżej mikrofonu.

Liderka zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska Justyna Wilczyńska-Baraniak:

Dziękuję za możliwość przedstawienia wniosków z raportu. Jako adwokat i lider zespołu prawnego do spraw cyberbezpieczeństwa w regionie EMEA kancelarii EY zajmuję się badaniem stanu regulacji z zakresu cyberbezpieczeństwa.

Spotykamy się dziś, aby rzeczywiście omówić ten niezwykle aktualny i ważny temat – wspólne ramy cyberbezpieczeństwa w Europie, czyli dyrektywę NIS2 oraz unijny 5G Toolbox, a przede wszystkim to, w jaki sposób Polska zamierza wprowadzić te narzędzia.

Punktem odniesienia do mojego dzisiejszego wystąpienia jest przygotowany przeze mnie wraz z moim zespołem europejskim raport, który zatytułowaliśmy: „Regulacje NIS2 i 5G Toolbox w Polsce. Analiza wdrożenia i porównanie z państwami Unii Europejskiej”, mając nadzieję, że ten raport, pokazujący w sposób obiektywny regulacje i podejście innych krajów, pomoże Polsce w przyjęciu właściwej drogi do wdrożenia dyrektywy NIS2 i usunie ewentualne obawy i rozbieżności zarówno biznesu, jak i przede wszystkim bezpieczeństwa cybernetycznego.

Pokrótkę opowiem o metodologii powstania raportu, wnioskach i kluczowych porównaniach wdrożenia NIS2 w poszczególnych krajach. Raport jest oczywiście dostępny, publiczny, tak że nie chciałabym tutaj zajmować więcej czasu. Można się z nim zapoznać.

Jeżeli chodzi o metodykę powstania raportu, raport został opracowany na podstawie dogłębnej analizy projektów ustaw oraz konsultacji legislacyjnych, które umożliwiały zrozumienie zmian i intencji regulacyjnych na poziomie krajowym i unijnym.

W opracowaniu wykorzystaliśmy porównanie rozwiązań stosowanych w 26 krajach Unii Europejskiej, co ilustrowaliśmy za pomocą tabel porównawczych wykresów pozwalających zobrazować różnicę w podejściu do wdrożenia regulacji. Analiza ta pozwoliła nam na identyfikację unikalnych cech polskiego podejścia oraz ewentualnych wyzwań wynikających z fragmentacji regulacyjnej na poziomie Unii Europejskiej. We wnioskach wskazaliśmy oczywiście różne podejście do implementacji tych regulacji w poszczególnych państwach.

Różnice dotyczą m.in. sposobu oceny dostawców i produktów. Niektóre państwa wdrażają formalne, szczegółowe procedury oceny, podczas gdy inne kierują się jedynie minimalnymi wymaganiami, co skutkuje odmiennymi poziomami rygorystyczności w zakresie weryfikacji.

Kryterium pochodzenia przy ocenie bezpieczeństwa. W niektórych krajach kryterium to jest kluczowym elementem oceny, natomiast w innych nie jest stosowane lub wdrażane w inny, mniej restrykcyjny sposób.

Różnice w klasyfikacji krytycznych elementów sieci. Podejścia różnią się między ograniczeniem wyłącznie do rdzenia sieci 5G a szerszym podejściem, które obejmuje również inne elementy takie jak radiowa sieć dostępowa RAN, co wpływa na zakres ochrony infrastruktury.

Mechanizmy wycofania sprzętu. Niektóre państwa przewidują możliwość natychmiastowego usunięcia sprzętu dostawców wysokiego ryzyka bez opcji wdrożenia środków naprawczych, co kontrastuje z bardziej elastycznymi rozwiązaniami przyjmowanymi w innych krajach, gdzie mogą być zastosowane działania naprawcze przed ostatecznym wycofaniem sprzętu.

Oczywiście główny wniosek naszego raportu wysuwa Polskę na tle Unii Europejskiej jako jeden z najbardziej restrykcyjnych modeli regulacyjnych. I skąd taki wniosek, bo to jest bardzo istotne.

Polska wdraża oba rozwiązania – dyrektywę NIS2 i 5G Toolbox w jednej ustawie. I to podejście rzeczywiście jest wyjątkowe i bardzo rzadko spotykane w Unii Europejskiej, gdzie zwykle te regulacje są wdrażane oddzielnie lub w ogóle w bardziej ograniczonym zakresie.

Rozszerzenie regulacji na wszystkie 18 sektorów objętych NIS2. Tak szerokie ujęcie wskazuje na bardzo rygorystyczne podejście do bezpieczeństwa, wykraczające poza standardowe wymagania przyjęte w innych państwach.

Wprowadzenie szczegółowych procedur oceny dostawców. Procedury te obejmują nie tylko aspekty techniczne, ale także geopolityczne, co dodatkowo podnosi poziom restrykcyjności.

Możliwość wycofania sprzętu dostawców wysokiego ryzyka. Polska przewiduje tutaj możliwość usunięcia sprzętu już w użyciu, co stanowi kolejny element wyróżniający jej model regulacyjny w stosunku do innych krajów.

Warto też tutaj dodać, że po ostatnim spotkaniu ministrów cyfryzacji Unii Europejskiej został podpisany Apel Warszawski w sprawie cyberbezpieczeństwa, w którym zawarto postulat skupienia się na zharmonizowanym podejściu i uproszczeniu wdrażania przepisów dotyczących cyberbezpieczeństwa oraz unikaniu fragmentaryzacji przepisów.

Chciałabym tutaj podsumować te wnioski z raportu i na potrzeby dzisiejszego spotkania jeszcze przypomnieć i wskazać, że dyrektywa NIS2 to następca pierwotnej dyrektywy NIS i w dużym skrócie ma ona zmusić państwa członkowskie do podniesienia poziomu odporności sieci i systemów informatycznych w sektorach uznanych za krytyczne dla gospodarki i funkcjonowania społeczeństwa. Lista tych sektorów jest długa – od energetyki i transportu, przez opiekę zdrowotną po badania naukowe. I zasadnicza idea brzmi: żaden kraj Unii Europejskiej nie powinien być najsłabszym ogniwem, bo wtedy cała wspólnota rzeczywiście traci.

I równolegle, gdy cyfrowy krwiobieg Europy przechodzi na technologię piątej generacji, Komisja Europejska wraz z agencją ENISA przygotowała 5G Toolbox. To jest zestaw zaleceń, jak ograniczać ryzyko związane z łańcuchem dostaw dla sieci 5G. Toolbox nie jest aktem powszechnie obowiązującego prawa. Jest to katalog środków technicznych i strategicznych, który państwa mogą, ale nie muszą wdrożyć. Zawiera m.in. sugestie, by dostawców wysokiego ryzyka, a więc takich, których produkty lub powiązania geopolityczne budzą wątpliwości, stopniowo eliminować z kluczowych elementów sieci.

Chciałabym w tym miejscu również spojrzeć na liczby. Spośród 26 państw Unii Europejskiej, aż 12 ograniczyło się do minimalnych wykluczeń, uznaje się za krytyczny wyłącznie rdzeń sieci 5G lub w ogóle nie klasyfikuje komponentów RAN. Trzy kraje stosują polityczne kryterium pochodzenia, pochodzenie spoza Unii lub NATO w ocenie dostawców, ale nie idą dalej w nakazach wycofywania sprzętu. Kolejne trzy państwa wprowadzają możliwe ograniczenia dotyczące komponentów 5G, nie przewidując jednak obowiązku ich usuwania. Dwa kraje wymagają zezwoleń lub zgłoszeń transakcji związanych z infrastrukturą 5G, a jedno, Niemcy, uznaje za krytyczne wyłącznie wąsko rozumiane systemy zarządzania radiową siecią dostępową i rdzeń sieci. Cztery państwa: Portugalia, Dania, Estonia i Litwa uznały za krytyczne wszystkie elementy RAN 3G, 5G, pasywne i aktywne oraz przewidują możliwość wycofania sprzętu.

Jedynie Polska planuje iść o krok dalej, obejmując restrykcjami wszystkie 18 sektorów, uznanych w dyrektywie NIS2. I to podejście jest najdalej idące w całej Unii. Taka rozpiętość pokazuje, że chociaż cel jest wspólny – ochrona sieci 5G – państwa różnią się co do arbitralności kryteriów, zakresu wyłączeń i mechanizmów egzekucji, co utrudnia spójną unijną strategię cyberbezpieczeństwa.

I teraz pytanie, dlaczego Polska chce tak szerokiego rozwiązania. Oficjalne uzasadnienie odwołuje się do specyfiki zagrożeń geopolitycznych w naszym regionie. Graniczymy z państwem agresorem, widzimy codziennie, jak wojna cybernetyczna przenosi się na infrastrukturę krytyczną i w tej narracji trudno oprzeć się wrażeniu, że ustawodawca woli zasadę ostrożności w wersji maksymalnej: lepiej zakazać z góry, niż później żałować. Jednak każde prawo, zwłaszcza tak rozległe, rodzi skutki uboczne.

Po pierwsze oczywiście koszty, o których tutaj już dzisiaj wspomniano. Operator, który zainwestował miliardy złotych w sprzęt wieloletni, może zostać zmuszony do jego wymiany w krótkim terminie.

Po drugie innowacyjność rynku. Jeżeli lista dostawców kurczy się do dwóch lub trzech globalnych graczy, wzrasta ryzyko oligopolu i przyspieszonego wzrostu cen.

Po trzecie wreszcie, harmonizacja w Unii. Regulacja, która tak bardzo odbiega od praktyk partnerów, może utrudniać transgraniczne projekty sieciowe, a także skomplikować współpracę w ramach jednolitego rynku.

Warto w tym miejscu zatrzymać się na chwilę przy samym pojęciu wysokiego ryzyka. Projekt polski definiuje je szeroko. Obejmuje zarówno kryteria techniczne: podatności sprzętu, możliwość wbudowania tylnych furtek, jak i nietechniczne: powiązania kapitałowe z rządem państwa spoza Unii lub NATO, doniesienia wywiadowcze, a nawet oceny dotyczące ochrony praw człowieka w kraju pochodzenia producenta.

Teoretycznie to dobrze. Bezpieczeństwo to nie tylko kod źródłowy, ale także przewidywalność otoczenia prawnego. Problem w tym, że tak szeroka definicja zostawia dużą uznaniowość organom administracji. Od decyzji politycznej do wykluczenia całej grupy produktów droga staje się bardzo krótka, a przedsiębiorcy tracą mierzalne kryteria pewności prawa. W średnim i długim terminie najważniejsze będzie znalezienie równowagi między suwerennością cyfrową a otwartością na globalną konkurencję. Paradoks bezpiecznej transformacji polega bowiem na tym, że całkowite odcięcie się od części dostawców może spowolnić wdrażanie najnowszych technologii, a tym samym przeciążyć inne elementy bezpieczeństwa, chociażby przeciążone, przedawnione systemy, które muszą działać dłużej, bo budżet pochłania wymiana sprzętu uznanego

za ryzykowny. W rezultacie rośnie nie tylko ryzyko szpiegostwa, lecz i awarii, i przestojów. Nie oznacza to wcale, że Polska nie powinna podejmować odważnych decyzji. Warto jednak pamiętać o zasadzie proporcjonalności. Być może lepszą drogą byłoby stopniowe, warunkowe wykluczanie najpierw w krytycznym rdzeniu, potem w aktywnych elementach RAN, a dopiero na końcu w pasywnych komponentach.

Na koniec pozostaje kwestia praktycznego egzekwowania prawa. Ustawa przewiduje, że minister odpowiedzialny za cyberbezpieczeństwo, w praktyce szef resortu cyfryzacji, będzie wydawał decyzje administracyjne w sprawie dostawców wysokiego ryzyka. Decyzja wejdzie w życie natychmiast, a odwołanie nie będzie wstrzymywało jej wykonania. To z jednej strony przyspiesza reakcję państwa na incydent, z drugiej budzi obawy o proporcjonalność, gdyż na rynku ICT mówimy o inwestycjach planowanych na dekadę w przód.

Szanowni państwo, próbując podsumować tę wielowątkową dyskusję, można użyć takiej metafory statku i portu. Unia Europejska jest portem, który stara się zbudować wspólne falochrony i to jest ta dyrektywa NIS2. Każde państwo cumuje w nim własny okręt z lokalnym ładunkiem. Polska zamierza doposażyć swój okręt w dodatkową podwójną burtę i własne wewnętrzne tamy. Może to uchronić nas przed sztormem, ale może też utrudnić zacumowanie obok innych statków, jeśli falochron okaże się za wąski. Kluczowa będzie więc sztuka manewrowania jak zachować szczelność, bariery bezpieczeństwa, a jednocześnie nie oddzielić się grubym murem od partnerów i innowacji, na których wszyscy zyskujemy.

Droży państwo, już rzeczywiście kończąc, cyberbezpieczeństwo nie jest chwilową modą ani zadaniem na jedno posiedzenie parlamentu. Jest to proces, w którym każde państwo i każda organizacja i w istocie każdy z nas odgrywa istotną rolę. Polskie ambicje i europejskie standardy absolutnie nie muszą być w sprzeczności. Mogą się uzupełniać, o ile będziemy gotowi do rzeczowego dialogu i do ważenia ryzyk na równi z ekonomią i innowacyjnością. Wierzę, że jest to możliwe i że dzisiejsza wymiana myśli i to, że mam dzisiaj przyjemność przedstawić wnioski z naszego szerokiego badania, jest właśnie krokiem w tym kierunku. Serdecznie dziękuję za uwagę.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję. Za chwilę przekazuję głos. Widzę, że pan dyrektor i pan prezes chcą zabrać głos. Oczywiście dyskusja będzie możliwa praktycznie bez ograniczeń.

Jest prośba m.in. od parlamentarzystów, żebyśmy ten raport – ja wiem, że on jest dostępny – ale jakbyśmy mogli przynajmniej dostać link do sekretariatu Komisji, to będę bardzo wdzięczny.

Liderka zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska Justyna Wilczyńska-Baraniak:

Oczywiście.

Prawnik w Zespole Własności Intelektualnej, Technologii i Ochrony Danych Osobowych w EY Polska Szymon Skalski:

Czyli wysłać na maila sekretariatu Komisji, tak?

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Na maila sekretariatu Komisji poproszę, tak.

Bardzo proszę, pan dyrektor. Proszę uprzejmie.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Bardzo dziękuję, panie przewodniczący. Mam pytanie o ten raport EY'a. Czy mogłaby pani mecenas powiedzieć, kto zlecił jego przygotowanie, kto jest faktycznym beneficjentem tego raportu?

Liderka zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska Justyna Wilczyńska-Baraniak:

Znaczący, powiem szczerze, że jak wskazałam, był opracowywany w ramach działań i w strukturach EY. Nie ma zlecającego.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Dziękuję, pani mecenas. Chciałbym sprostować i wyjaśnić kilka rzeczy. Właśnie to jest to wyzwanie związane z dyskutowaniem o projekcie KSC, ponieważ podmioty cieszące się taką estymą jak EY niestety przekazują szereg nieprawdziwych informacji.

Pierwszą nieprawdziwą informacją, takim sztandarem osób zwalczających tę superważną regulację jest fakt, że Polska i inne kraje nie są zobowiązane do wdrożenia Toolbox 5G. W tej kwestii wielokrotnie komisja jednoznacznie wypowiadała się, również w związku z wdrożeniem Europejskiego kodeksu łączności elektronicznej, jest prawny obowiązek nałożony na państwo, żeby wdrożyć Toolbox 5G. To nie należy do swobody zdecydowania. Po pierwsze.

Po drugie był taki zarzut, że grozi nam wdrożenie regulacji odbiegających od tych, które zostały wdrożone w innych państwach. Pani mecenas, te wszystkie przesłanki, których część pani przywołała, one wynikają ze skoordynowanej oceny. Byli w to zaangażowani eksperci państw członkowskich, europejska agencja do spraw cyberbezpieczeństwa. Proszę, nie posługujemy się dokumentami i tezami wybiórczo. Naprawdę bardzo wiernie odnosimy się do tych przesłanek. Mamy bardzo sformalizowaną procedurę, pewnie najbardziej sformalizowaną, która zawiera najwięcej bezpieczników, najwięcej podmiotów zaangażowanych, decyzyjnych, żeby wypowiedzieć się na poszczególne tematy, komponenty tej bardzo złożonej procedury, bo tak ona jest zaprojektowana. Jest kolegium, wypowiadać się mają służby, poszczególni ministrowie co do swojej właściwości i ma być powołany zespół ekspertów. Naprawdę wskazywanie czy chociażby sugerowanie, że my poszliśmy drogą na skróty w sposób nierzetelny czy odbiegający, jest bardzo nie fair.

A ze względu na gravitas regulowanych spraw należałoby zadać kolejne pytanie, komu tak naprawdę zależy na tym, żeby, w mojej ocenie, w tak niewłaściwy sposób prezentować te regulacje zawarte w ustawie.

Odnosząc się do 18 sektorów, wdrażając pierwsze KSC, Polska przyjęła szerszą definicję incydentu. Zgodnie z pierwszą dyrektywą NIS, incydem jest coś, co ma wpływ na bezpieczeństwo systemów teleinformatycznych. Ekspertci wdrażający powiedzieli wtedy: „Słuchajcie, należy objąć także zdarzenia, które mogą mieć wpływ”, żebyśmy je rejestrowali, żebyśmy je raportowali, żeby można segregować te dane, żeby pobudzić te podmioty krajowego systemu cyberbezpieczeństwa, czyli de facto te podmioty, na które są nałożone obowiązki regulacyjne, ważne do funkcjonowania państwa, rozszerzyć tę definicję. Co się okazało w przypadku przeglądu dyrektywy NIS2? – Polska miała rację.

Oczywiście dyskutowaliśmy ówczesnie, że to jest szersze podejście, teraz już jest definicja cyberzagrożenia i Komisja Europejska, państwa członkowskie przyznały rację Polsce, naszym ekspertom, czyli powinno być tak zaadresowane, aby również potencjalne zdarzenie miało wpływ na regulację.

Panie przewodniczący, czy może panie i panowie posłowie, kwestia backdoorów w falownikach. Będę bazował wyłącznie na informacjach dostępnych publicznie. Zagrożenie dla bezpieczeństwa niektórych służb, to znaczy nie wiadomo w jaki sposób, gdzie są przekazywane dane, gdzie są trzymane dane, w jaki sposób można kontrolować. To ma wpływ na bezpieczeństwo państwa. Możliwość przekazywania przez ukryte moduły komunikacyjne informacji na przykład z dronów, które wykonujemy do infrastruktury krytycznej. Pani mecenas państwu tego nie powie, bo zasadą w Unii Europejskiej i z Komisją jest tak, że dopóki coś jest draftem, to się go nie upublicznia. To znaczy, że dyskutujemy nad tym pomiędzy państwami członkowskimi. Kiedy dokumenty są sfinalizowane, powstają rekomendacje, wszyscy państwo możecie zapoznać się z nimi publicznie.

Ja powiem, że w wielu tezach jest wskazane, że te zagrożenia, które dotyczą Toolbox ekstrapolują na inne sektory gospodarki. Mają wpływ oczywiście na energetykę, mają wpływ na szereg innych rozwiązań. Takie też łączenie dwóch ważnych rzeczy z jednej strony instytucja prawna, możliwość działania prawem w tych ramach, które proponujemy, a podjęcie właściwych, odpowiednich działań, to są dwie różne rzeczy. Znaczą te raporty, które pochodzą od Unii Europejskiej i jasno wskazują, które państwa wdrożyły Toolbox 5G, czyli mają ramy prawne do działania – my niestety nie mamy – i również część krajów członkowskich, ponad 10 krajów członkowskich zdecydowało się, żeby podjąć środki, czyli podjąć to, co jest opisane w tej procedurze dostawców wysokiego ryzyka w nowelizacji ustawy w formie decyzji administracyjnej w przypadku zaistnienia tych przesłanek związanych z naruszaniem podstawowego interesu w zakresie bezpieczeństwa państwa. To znaczy równie dobrze można było przygotować analizę, z której wnioski byłyby zupełnie odmienne, to znaczy, że to my gwarantujemy największe bezpieczniki z zakresu praworządności.

Szanowni państwo, panie posłanki, panowie posłowie są państwa, gdzie po prostu wiceminister wydaje akt, po prostu miękki dokument i on ma taki skutek, że zobowiązuje państwa

w związku z bezpieczeństwem narodowym do wycofania sprzętu. My mamy procedurę administracyjną, w której można się wypowiedzieć, zająć stanowisko, gdzie są strony postępowania, naprawę. Znaczą, jeżeli chodzi o te gwarancje procesowe, które my zapewniamy, to porównawczo wypadamy bardzo, bardzo rzetelnie. Ale tego niestety nie mogliśmy usłyszeć we wnioskach. Dziękuję, panie przewodniczący.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo. Proszę, pan prezes Kanownik.

Prezes Zarządu Związku Cyfrowa Polska Michał Kanownik:

Dziękuję bardzo, panie przewodniczący. Szczerze mówiąc, nie wiem, od czego zacząć, bo jak słuchałem wniosków pani mecenas, to momentami miałem wrażenie, że idziemy w kierunku żartu, a momentami czegoś, co mnie przeraża. Ale spróbuję być poważny. To będzie bardzo trudne, ale spróbuję być.

Jeżeli pani mecenas mówi z wniosków, że Polska wdraża tym projektem najbardziej restrykcyjne prawo z zakresu cyberbezpieczeństwa w Europie, to rozumiem, że wszyscy przykłaśniemy brawo i pochwalimy polski rząd za to, że robi wszystko, żeby być najbezpieczniejszym krajem w Europie. Chyba że wniosek pani mecenas miał na celu pokazanie, że to źle, że jesteśmy restrykcyjni w zakresie naszego bezpieczeństwa narodowego, ale następnie pani mecenas sama potwierdziła, że z uwagi na choćby graniczenie z krajem frontowym, atakami, które mamy codziennie, to jest oczywista oczywistość, jak mawiał klasyk, że to musi się stać bez żadnego kompromisu w tym zakresie.

Pani mecenas powołuje się na to, że w projekcie mamy bardzo restrykcyjne zapisy odnośnie do wycofywania sprzętu, który państwo polskie uznaje za sprzęt dostawców wysokiego ryzyka. Szanowni państwo, mówimy o sytuacji, w której służby państwa uznają, że coś jest dla nas niebezpieczne. I ten projekt ustawy na ten moment zakłada, że jeszcze przez cztery lata ten sprzęt, nadal niebezpieczny, może pracować. To, gdzie tu restrykcyjność?

Pani mecenas na końcu poszła w poetykę portową, to ja może trochę mniej poetycko, ale w przenośni: jeżeli w swojej kuchni znajdę karaluchy, to nie wyczyszczę tylko jednej szuflady, jednej szafki, tylko całą kuchnię i to jak najszybciej. A tymczasem pani mecenas sugeruje, że pomimo że wiemy, że ktoś nam zagraża, mamy pozwolić mu działać, a może poprawi się za rok czy dwa i jednak będzie już dobry. No nie, to kompletnie nie ma logiki. Jeżeli wiemy, że ktoś nam zagraża, to natychmiast powinniśmy go usunąć. Więc ta ustawa jest moim zdaniem za mało restrykcyjna w tym zakresie, bo pozwala na to, żeby komponenty, które są niebezpieczne dla państwa polskiego, funkcjonowały w sieci telekomunikacyjnej. Te przepisy powinny być... jak najszerzej, bo nie tylko kwestia telekomunikacji, ale każdego aspektu naszej gospodarki powinna podlegać tym jak najbardziej restrykcyjnym przepisom.

Jeżeli już nawet sama Komisja Europejska, która zawsze jest powściągliwa w tym zakresie, wprost zakazuje używania odpowiednich sprzętów przez Komisję Europejską, przez członków Parlamentu Europejskiego, to co my jeszcze próbujemy doszukiwać się w Europie, że może nie bądźmy aż tak radykalni w zakresie naszego bezpieczeństwa. Pani mecenas, nie ma czasu i miejsca na kompromisy, jeśli mówimy o naszym bezpieczeństwie, a cyberbezpieczeństwo jest kluczowym elementem w tym zakresie. Nie mówimy tylko wyłącznie o jakiejś hipotetycznej sytuacji. Mówimy o realnym zagrożeniu, które mamy każdego dnia i to nie pojedyncze przypadki, tylko dziesiątki, setki i tysiące takich ataków. Przykłady naprawę mamy w całej Europie, możemy pokazywać, choćby rumuński ostatnio. To nie jest nagle, że ktoś tam nagle znikąd spowodował zagrożenie dla demokracji rumuńskiej, tylko konkretne, technologiczne rozwiązania. To właśnie narzędzia prawne pozwalają reagować w odpowiednim czasie i miejscu, żeby powściągnąć takie próby.

Panie przewodniczący, chyba brakuje mi słów, żeby wyrazić, jak nie zgadzam się z wnioskami z tego raportu.

Raczej z jednym wnioskiem się zgadzam i dziękuję pani mecenas za to, że on padł. Polska wdraża jedną z najbardziej restrykcyjnych regulacji w zakresie cyberbezpieczeństwa. I super, że to robi.

Panie dyrektorze, jako biznes liczymy, że te przepisy wejdą jak najszybciej w życie właśnie w takiej restrykcyjnej formie, żebyśmy byli najlepiej zabezpieczonym krajem w Europie.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję. W odniesieniu do tej wypowiedzi pani mecenas, bardzo proszę.

Liderka zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska Justyna Wilczyńska-Baraniak:

Proszę...

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Proszę włączyć mikrofon.

Liderka zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska Justyna Wilczyńska-Baraniak:

Tak, ad vocem. Jeżeli pan wskazuje, że jako polski biznes państwo dziękujecie za tak restrykcyjną regulację, to gdzie są ekonomiczne skutki analizy wdrożenia tej regulacji i gdzie są stanowiska podmiotów, których ta regulacja będzie dotyczyć odnośnie do wskazanych procedur.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo. Proszę, pan mecenas.

Ekspert ds. telekomunikacji Polskiej Izby Komunikacji Elektronicznej Tomasz Bukowski:

Dziękuję, panie przewodniczący. Nie mogę się zgodzić z moim przedmówcą, że biznes jest zachwycany najbardziej restrykcyjnymi rzeczami. Będąc dzieckiem, miałem już do czynienia z siecią telekomunikacyjną superbezpieczną w latach 80., gdzie po podniesieniu słuchawki słyszało się: „rozmowa kontrolowana”, więc możemy oczywiście wrócić do czegoś takiego. Bezpieczeństwo tak, ale również bezpieczeństwo gospodarcze.

Mówiąc wprost, dlatego z tą ustawą idzie tak trudno, bo polscy przedsiębiorcy nie udźwigną tych regulacji. Po prostu nie udźwigną. My możemy powyrywać groźne urządzenia ze skrzynek i zamontować tam cegły, bo tylko na to nas będzie stać. I będzie to dotyczyło również wszystkich sieci telekomunikacyjnych wybudowanych z funduszy unijnych, złośliwie mogę powiedzieć, również sieci edukacyjnej OSE nadzorowanej przez NASK, która nagle też stanie się niebezpieczna, a też jest na komponentach, zresztą na wyraźne żądanie rządu, określonych firm.

Powtarzam, że rozumiem punkt widzenia ministerstwa, że chodzi im o bezpieczeństwo. Nam chodzi również o bezpieczeństwo gospodarcze i o to, aby to było możliwe do zastosowania. Mamy przykłady, w jaki sposób zastosowano ten mechanizm w Stanach Zjednoczonych, gdzie przedsiębiorcy amerykańscy nie udźwignęli tego mimo wsparcia finansowego ze strony rządu amerykańskiego. Projekt, który miał trwać nie więcej niż dwa lata, jest już mocno wydłużony. Trwa piąty rok, po ciężkich walkach między Federalną Komisją Łączności a Kongresem o dodatkowe finansowanie, mówimy tu o miliardach dolarów, podczas gdy u nas dochodzi się do tego, że jest to coś, co ma być finansowane tylko i wyłącznie przez przedsiębiorców, a nie z budżetu.

Prosiłbym jeszcze o niemieszanie pojęć, mówiąc o bezpieczeństwie urządzeń i oprogramowania z cyberhigieną i zagrożeniem rumuńskim, bo pod tym względem, czyli wdrożenia Digital Services Act, Polska jest w jeszcze gorszej sytuacji niż przy wdrażaniu NIS2. I tu są też poważne problemy, obawy. Ja mogę tylko podać przykład, że w zakresie cyberhigieny w Polsce jest przyjęty systemowy chaos. Dopiero sektor prywatny próbuje wymusić na rządzie tworzenie jednego, szczelnego systemu blokowania identyfikowania treści niebezpiecznych. Więc nie mieszałbym do tego wdrożenia NIS2, bo to jest zupełnie inna dyrektywa i tutaj pionierami wdrożenia tego tak naprawdę jest sektor prywatny. Dziękuję bardzo.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję. Pan dyrektor, proszę bardzo.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Pani mecenas, stanowiska wszelkich organizacji są publikowane na stronach Rządowego Centrum Legislacji. Zakładałem, że pani mecenas, przygotowując raport, wie, gdzie można znaleźć opublikowane i przygotowane stanowiska.

Natomiast o czym ja nie powiedziałem, a pan prezes powiedział w swojej wypowiedzi, to terminy wycofania sprzętu. Termin podstawowy dotyczący rdzenia sieci piątej generacji, czyli dotyczący tych pozostałych sektorów, wynosi siedem lat, co pokrywa się po pierwsze z cyklem życia produktów ICT. Czyli pomimo tego, że identyfikujemy zagrożenia podstawowych interesów

państwa, to tu już jakby w tym core rozwiązania wyważone są te interesy podmiotów prowadzących działalność gospodarczą, to znaczy w tym terminie. On i koresponduje z cyklem życia produktów ICT i z drugiej strony, chyba pani mecenas nie powiedziała, ale też jest jednym z dłuższych terminów, które obowiązują w krajach unijnych. Więc to chyba też warto było powiedzieć, wtedy to podsumowanie tych wniosków na pewno nie miałoby takiego charakteru stricte tendencyjnego. Dziękuję.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo i proszę o merytoryczne...

Liderka zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska Justyna Wilczyńska-Baraniak:

Ale...

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Ale teraz pan poseł Bliźniuk. Bardzo proszę.

Poseł Paweł Bliźniuk (KO):

Dziękuję za możliwość wypowiedzi. Przysłuchuję się tej dyskusji. Chciałem podziękować za wszystkie głosy, bo dla nas jako członków Komisji pewnie są bardzo cenne, ale już nie wchodząc w szczegóły tej wymiany zdań, to państwa dyskusja i te argumenty, które padają, tylko podkreślają wagę tych regulacji. Stąd też ponawiam kwestię terminu, kiedy dostaniemy ten projekt, bo z naszej perspektywy jako parlamentarzystów to jest na razie taka rozmowa na temat przedłożenia, które jeszcze nie jest przedmiotem naszego bezpośredniego, podkreślę, bezpośredniego zainteresowania jako Sejm, czyli projektu ustawy. To po pierwsze.

Po drugie rozumiem, że w tym raporcie, o którym też rozmawiamy, mówiąc o tym czynniku geopolitycznym, mówimy o kwestiach zagrożenia najbliższego sąsiedztwa, faktu, że jesteśmy poddawani atakom cybernetycznym w rekordowej liczbie, jeżeli patrzymy na wszystkie państwa Unii, ale brakuje mi jeszcze jednego elementu, czyli jakiejś refleksji, która towarzyszy bądź wychodzi naprzeciw aktom prawnym, które w Stanach Zjednoczonych były u podstaw AI diffusion act, który wiemy, że nie wejdzie w życie, będzie zmieniony, natomiast tej filozofii dotyczącej poszerzenia zakresu definicji bezpieczeństwa i tu jest kwestia w ogóle zdolności rozwojowych państwa w najbliższych latach. Oczywiście ta filozofia regulacji ma zostać zmieniona, taka jest zapowiedź władz amerykańskich, ale kwestie cyberbezpieczeństwa przy tej dotychczasowej filozofii były aspektem fundamentalnym z punktu widzenia w ogóle możliwości rozwojowych naszego państwa. Stąd też taki sygnał, że projektujemy rozwiązania ustawowe, które mają nas zabezpieczyć, jest też sygnałem w kontekście geopolitycznym, istotnym z tego punktu widzenia. Nie wiemy jeszcze, bo też mamy tylko bardzo lakoniczną informację ze strony administracji prezydenta Trumpa, jak mają regulować teraz te kwestie związane z ograniczeniami eksportu czy też inwestowania w rozwój nowych technologii, w tym sztucznej inteligencji, w państwa, które są uznawane za państwa sojusznicze, partnerskie dla Stanów Zjednoczonych. Patrząc na dotychczasową praktykę, być może ta zmiana będzie głębsza, ale ta kwestia bezpieczeństwa była fundamentalna. Ta definicja bezpieczeństwa w tych aktach, która była u podstaw decyzji Departamentu Handlu dotyczącej ograniczeń, cały czas jakby poszerzała swój zakres i naszą odpowiedzialnością również jest kwestia dobrych regulacji w zakresie cyberbezpieczeństwa. Myślę, że mimo zmiany w ogóle filozofii regulacji, to ta istota, ta treść czy być może ta filozofia działania, może nie sama forma regulacji, pozostanie najprawdopodobniej niezmienną. Nie będzie ogólnych restrykcji, tylko administracja Stanów Zjednoczonych będzie patrzyła w jaki sposób my realizujemy kwestie związane z bezpieczeństwem w praktyce.

Tego mi brakuje w tym raporcie, jeżeli mówimy o wątku geopolitycznym i wydaje mi się, że ten temat również jest istotny z punktu widzenia bezpieczeństwa gospodarczego państwa polskiego, jego konkurencyjności gospodarki i naszych możliwości rozwojowych w niedalekiej przyszłości.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję, panie pośle. Proszę, pani mecenas.

Liderka zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych w EY Polska Justyna Wilczyńska-Baraniak:

Jedno pytanie dotyczące zakresu 5G Toolbox, które dotyczy sektora telekomunikacyjnego, wdrażanie państwo do ustawy o krajowym systemie cyberbezpieczeństwa, która dotyczy 18 sektorów.

Nie rozumiem i prosiłabym o wyjaśnienie, dlaczego rozwiązania 5G Toolbox mają objąć inne sektory niż sektor telekomunikacyjny. Czy, bo tak rozumiem, świetnie, mamy przyklasnąć, Polska ma najbardziej rygorystyczną regulację, świetnie i chwalmy za to Polskę. Dlaczego? I to jest jedno moje pytanie.

Dlaczego rozciągamy 5G Toolbox na wszystkie inne sektory niż sektor telekomunikacyjny? Czy sprawdziliście na przykład w ochronie zdrowia jakie są komponenty? Czy w ogóle są zamienniki w przypadku wycofania sprzętu? Jakie to będzie miało skutki dla tego sektora?

Ja miałam konferencję, chociażby z sektorem energetycznym, gdzie zrobiliśmy głosowanie i powiedzieli, że sektor energetyczny to w ogóle należałoby dać do odrębnej ustawy. Również jest raport na naszej stronie Portal Prawny NIS2.

Naprawdę przysłałam tutaj – dziękuję bardzo za zaproszenie – będąc otwarta na dyskusję merytoryczną, a czuję się trochę jak zbity pies. Naprawdę zachęcam do merytorycznej dyskusji, refleksji nad argumentami merytorycznymi, a nie tylko na tym, że brawo, bo rozwiązania Polski są rygorystyczne.

Ja doradzam wielu podmiotom międzynarodowym, które chcą wdrażać technologie. Mamy chociażby sektor finansowy, gdzie zawsze przedsiębiorcy globalni łapią się za głowę, bo podejście choćby regulatora zawsze w Polsce jest najsurowsze i rygorystyczne. Zawsze jesteśmy tą czerwoną mapą. Czy naprawdę musimy nią być? Czy musimy być tak ambitni? Jeżeli musimy, to ja poproszę o konkretne argumenty, których nadal nie znam, dlaczego 5 G Toolbox rozciągamy na 18 sektorów?

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję, pani mecenas. Proszę się tak nie czuć, bo nikt nie miał chyba takiego zamiaru.

Ponawiam prośbę właśnie o merytoryczną dyskusję. Może mniej tych określeń tego typu. Bardzo proszę, pan dyrektor.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Bardzo dziękuję, panie przewodniczący. O wpływie, dlaczego to jest istotne, żeby objąć 18 sektorów, mówiłem przed chwilą. Ale chciałbym, żeby pani mecenas również czuła się komfortowo, więc przypomnę.

Te zagrożenia, które wynikają z działania sieci telekomunikacyjnej, ekstrapolują na inne sektory. To znaczy może być tak, że ze względu na brak sieci telekomunikacyjnej, mamy wpływ na sektor energetyczny. Może być na przykład tak, że falowniki mają komponenty niebezpieczne, że tak naprawdę nie wiemy, gdzie są przekazywane dane, w jaki sposób może zostać przejęta kontrola. To dotyczy odnawialnych źródeł energii, fotowoltaiki. To są bardzo poważne problemy, o których może pani mecenas przeczytać w przestrzeni publicznej. Są oczywiście dyskusje na temat dronów, są możliwości też np. zawarcia modułów komunikacyjnych niezgodnie ze specyfiką. A wszystkie te zagadnienia związane z bezpieczeństwem łańcucha dostaw zostały zaadresowane właśnie przez Unię Europejską w takim obowiązku zapewnienia bezpieczeństwa łańcucha dostaw podwykonawców, więc tak naprawdę podmioty objęte tą regulacją to nie tylko będą te podmioty kluczowe, podmioty ważne, mówiąc żargonem tej ustawy, które będą miały obowiązki, ale też często ich kontraktorzy, podwykonawcy, bo te ataki w cyberprzestrzeni to mogą być właśnie ataki na przykład na dostawcę, na mniejszy podmiot, który dostarcza kluczowych usług dla innego podmiotu. I sam fakt, że te zagrożenia już nie dotyczą wyłącznie sieci piątej generacji, coraz jaśniej wybrzmiewają. To znaczy to, o czym mówi pani mecenas, że ta regulacja jest najbardziej restrykcyjna, to z biegiem czasu jestem przekonany co do tego, że Unia Europejska też podejmie działania w tym zakresie i na pewno zostaną przeprowadzone analizy, czy te działania były adekwatne i proporcjonalne. Czyli wyłącznie skupienie się tak naprawdę na największym zidentyfikowanym zagrożeniu, czyli sieciach piątej generacji.

Dlatego jestem przekonany, że co do możliwości zabezpieczenia łańcucha dostaw, co wynika z dyrektywy NIS2, jest potrzebne takie szersze, cross sektorowe podejście, żebyśmy zadbali o podstawowe interesy w zakresie naszego bezpieczeństwa, bezpieczeństwa państwa do tego, żebyśmy mogli zadziałać w przypadku stwierdzenia o takim charakterze zagrożeń. Niestety, jeżeli nie będziemy mieli narzędzia i państwo nie zadziała, to obawiam się, że konsekwencje takich zaniechań dotkną całe społeczeństwo, nas wszystkich, a także państwo jako całość.

Pani mecenas, co do tego zamówienia raportu, to państwo prowadzicie działalność biznesową. To znaczy celem biznesu jest prowadzenie działalności gospodarczej, czyli prowadzenie zysku. Czy pani mecenas chce powiedzieć, że takie raporty powstają w ramach jakiegoś działania

o charakterze non profit, wsparcia? Rozumiem, że dla firmy, przedsiębiorcy, u którego pani pracuje, jednak nadrzędny ponad wszystko jest ten cel biznesowy, nawet jeżeli to zamówienie formalnie nie zostało złożone, tak jak pani mecenas oświadczyła podczas tego posiedzenia.

Nie chciałbym, żeby pani mecenas się źle czuła, a nawet żeby zwierzęta się źle czuły, żeby absolutnie ludzie nie byli bici, przyrodzona godność człowieka, a zwierząt również.

Dziękuję, panie przewodniczący.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję bardzo. Czy ktoś z państwa chciałby zabrać głos? Proszę uprzejmie.

Prawnik w Zespole Własności Intelektualnej, Technologii i Ochrony Danych Osobowych w EY Polska Szymon Skalski:

Dzień dobry państwu, szanowna Komisjo, wydaje mi się, że tak naprawdę od czegoś takiego powinniśmy zacząć, bo też nie wiem, czy wszyscy państwo mają cały ten kontekst legislacyjny, o którym ja też miałem z panem dyrektorem szansę dyskutować na różnych webinarach, które organizowało Ministerstwo Cyfryzacji. Nie wiem, czy pan dyrektor pamięta, ja w trakcie tych webinarów zadawałem dość dużo pytań.

To wygląda tak – to, co pan dyrektor mówił odnośnie do tych procedur, w tym momencie ze strony Ministerstwa Cyfryzacji, właśnie przy okazji jednego z tych webinarów, pojawiła się taka komunikacja dotycząca mitów. Tam na kolejnych slajdach było pokazywane kilka mitów. Jednym z tych mitów, i też tym, co pan dyrektor dzisiaj powiedział, jest to, że Polska tą procedurą dostawców wysokiego ryzyka nadinterpretuje kwestie związane z NIS2, dodaje coś do NIS2 zgodnie z tym, co Ministerstwo Cyfryzacji proponuje, to po prostu bezpośrednio wynika z tego, co NIS2 każe nam transponować.

Jak to wygląda tak czysto prawniczo z perspektywy analizy tych dwóch aktów prawnych? W NIS2 ta procedura znajduje się w art. 90, 91 w art. 21 ust. 3 i w art. 22. W Polsce ta procedura, o której mówimy, znajduje się w art. 67b tego projektu.

Teraz tak, ta procedura na poziomie unijnym, zresztą zgodnie z nazwą tzw. skoordynowana ocena ryzyka łańcucha dostaw, dotyczy właśnie łańcucha dostaw, czyli na poziomie unijnym grupa współpracy to jest taki organ polityczny, który składa się z podmiotów delegowanych, z osób delegowanych przez państwa członkowskie ze wsparciem ENISY i Komisji Europejskiej, przeprowadza skoordynowane szacowanie ryzyka i na podstawie tego wydaje coś takiego jak 5G Toolbox. 5G Toolbox, żeby rozwiązać parę mitów, już trzymając się tej terminologii, nie był tak wydany. On był wydany na podstawie, moim zdaniem, troszeczkę wątpliwego mechanizmu, który komisja stosuje, czyli po prostu oni wydali taką wewnętrzną regulację, na podstawie której potem zrobili 5G Toolbox. To już pomijając to, bo jeżeli chodzi o 5G Toolbox, ta dyskusja już jest raczej zamknięta. I to jest procedura na poziomie unijnym. Zgodnie z tą procedurą mogą być zidentyfikowani dostawcy wysokiego ryzyka w obrębie określonego łańcucha dostaw. To jest zamknięta procedura. I tu efektem potencjalnym poza tymi wytycznymi dla państw członkowskich jest zidentyfikowanie dostawcy wysokiego ryzyka.

Teraz mamy procedurę polską inicjowaną przez Ministerstwo Cyfryzacji, opiniowaną przez Kolegium do Spraw Cyberbezpieczeństwa. Tam jest dość długi tryb tej procedury rozpisany bardzo szczegółowo, z której też wychodzi dostawca wysokiego ryzyka, ale to jest inny dostawca wysokiego ryzyka, przynajmniej moim zdaniem. Rozmawiamy tu o projekcie, możemy sobie troszeczkę pozwolić też na taką interpretację prawną tego. To jest inny dostawca wysokiego ryzyka niż ten unijny, ponieważ dostawca unijny wysokiego ryzyka jest w UKSC oczywiście, bo musi być. On jest tak samo jak we wszystkich innych państwach. Ja jako autor tego raportu miałem szansę, też trochę wątpliwą radość, przeczytać wszystkie projekty, które tam były w tych różnych językach, po tłumaczeniach i zazwyczaj to jest zrobione we wszystkich państwach dokładnie tak samo, czyli tam, gdzie mamy wymogi w zakresie cyberbezpieczeństwa, na końcu – i to odpowiednik art. 21 ust. 3 NIS 2 – dodaje się takie zdanie, że w ramach realizacji w szczególności art. 21 ust. 2d NIS2, czyli tego, który wymaga zapewnienia bezpieczeństwa łańcucha dostaw, podmioty muszą respektować wyniki skoordynowanego szacowania ryzyka. I każde państwo równiutko przerzuciło ten artykuł do ustawy implementującej. Bardzo dobrze, bo w ten sposób implementujemy tę procedurę skoordynowanego szacowania ryzyka, czyli przy kontroli podmiotu sprawdzamy, czy jest skoordynowane szacowanie ryzyka, czy jest ten Toolbox, który jest tego efektem i czy podmiot też to wdrożył. I to jest ta procedura unijna. A ta procedura 67b to jest ten dodatek polski, przynajmniej w mojej interpretacji tych przepisów.

I teraz, podsumowując całą tę wypowiedź, co było też tak naprawdę moim celem w tym raporcie, jak państwo będą mieli przyjemność, mam nadzieję, przeczytać ten raport, on jest dość specyficzny, bo składa się z dość krótkiej części, o której teraz tutaj była cała ta dyskusja. To jest około 12–13 stron takiego wprowadzenia do tej problematyki i to jest rzeczywiście ta część dyskusyjna, która też podsumowuje te argumenty zgłaszane przez biznes. I to wszystko.

Potem mamy dwadzieścia parę-trzydzieści stron tabeli. Ta tabela dotyczy każdego kraju po kolei, gdzie mamy zadane takie same pytania do każdego kraju. Mamy napisane, to jest w tych aktach prawnych i tak naprawdę najważniejszą częścią tego raportu i też naszą intencją w ramach tego raportu było takie suche pokazanie tych przepisów, że po prostu w tych innych krajach takie przepisy są lub takich przepisów nie ma. Konkluzją z tego, tak naprawdę najważniejszą jest to, że są różnice między tymi państwami. W niektórych jesteśmy mniej rygorystycznie, w niektórych jesteśmy bardziej rygorystyczni.

Jeżeli chodzi o tę jedną procedurę, ona została dodana całkowicie autorsko. To jak my to oceniamy, to już jest kwestia analizy gospodarczej, tak jak tutaj państwo mówili, ekonomicznej, politycznej, tak naprawdę geopolitycznej z perspektywy bezpieczeństwa i to jest jasne. I to będzie robione na poziomie Sejmu, Senatu, potem poprawek tego wszystkiego. To, co my chcieliśmy zrobić, to tylko pokazać, że to jest ten mechanizm, który trzeba troszeczkę wyciągnąć przed nawias tej ustawy i analizować tak naprawdę osobno.

Więc to tak, żeby troszeczkę też sklaryfikować. Przepraszam, że tak długo, ale ten kontekst legislacyjny, też prawny tego całego zagadnienia.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Jasne. Bardzo dziękuję. Proszę uprzejmie.

Ekspert ds. telekomunikacji Polskiej Izby Komunikacji Elektronicznej Tomasz Bukowski:

Dziękuję, panie przewodniczący. Może już tak kończąc. Mowa tu jest o wielu raportach, m.in. też unijnych. My jako przedsiębiorcy mamy przede wszystkim w głowie raport Draghiego o dwóch skutkach nadregulacji.

Pierwsze to uderzenie w rynek jednolity i tutaj będzie uderzenie w rynek jednolity, bo będą problemy z naszymi partnerami unijnymi, którzy będą chcieli prowadzić działalność gospodarczą na terenie Polski przy użyciu swoich sprzętów, swoich oprogramowań i nie będą rozumieli, dlaczego nie wolno im tego robić, jeżeli w ich własnych krajach jest to dopuszczalne. A drugie oczywiście będzie to uderzenie w konkurencyjność polskich firm. To jest jedna kwestia.

Druga kwestia odnośnie do entuzjazmu w zakresie bezpieczeństwa. Bodajże w 2006 r. dokładnie na tej sali mieliśmy już dyskusję na temat nadregulacji Polski w zakresie bezpieczeństwa w zakresie retencji danych obywateli przez operatorów i przez służby na rzecz służb. Podczas gdy w Unii Europejskiej kształtowała się wtedy praktyka retencji danych przez okres maksymalnie dwóch lat, obecni wówczas politycy stwierdzili, że Polska będzie lepsza i będzie to okres pięciu lat, chociaż wychodzili z założenia, że najlepiej byłoby, gdyby było na zawsze. I to też było bezpieczeństwo, które pokazywało właśnie, że pewne rzeczy trzeba jednak wziąć również pod uwagę nawet przy zapewnieniu bezpieczeństwa, również jakieś inne wartości. W tej chwili mamy do czynienia z wartościami gospodarczymi. W kwestii retencji danych zeszliśmy do jednego roku i jakoś z tego powodu nie staliśmy się mniej bezpiecznym krajem, więc ja też nie uważam, że wprowadzenie standardowych unijnych regulacji spowoduje zagrożenie bezpieczeństwa naszego kraju. Estonia nie wprowadza takich regulacji, podobnie jak Łotwa, mimo że ciągle są celem ataków, Rumunia również jest krajem frontowym, Finlandia teraz też staje się krajem frontowym, więc nie jesteśmy jedyń, ale tylko u nas jest tłumaczenie, że wychodzimy przed szereg.

Kolejna kwestia, o której chciałem powiedzieć, to jest permanentne wymaganie przerzucania bezpieczeństwa na sektor prywatny, podczas gdy on już sam z siebie jest bardzo odporny, co zresztą pokazują dokumenty ENISY w energetyce, w telekomunikacji, w bankowości, podczas gdy najmniej bezpiecznym sektorem jest administracja. I nie widzę ani w tej ustawie, ani w innych działaniach poprzedniego rządu jakichkolwiek prób wymuszenia na samej administracji wprowadzenia bezpieczeństwa.

Ja mogę podać wyjątkowo perfidny przykład związany z tym, co będzie na następnym posiedzeniu Komisji, a więc z wysyłanymi SMS-ami, podszywającymi się podróże instytucje, kiedy Polska wyszła przed szereg, ale stworzyliśmy jeden z najlepszych systemów antysmishingowych. OK, był tylko jeden problem. Sieci telekomunikacyjne były do tego przygotowane, NASK był do tego przygotowany, UKE było do tego przygotowane, tylko podmioty publiczne, które powinny

zgłaszać swoje nadpisy w celu ich identyfikacji i zapobieganiu podszywaniu i oszustwom, tego nie zrobili. I do dziś 1,5 roku ustawy i nadal instytucje publiczne tego nie zrobiły.

Więc ja nie widzę pracy w zakresie bezpieczeństwa po stronie rządowej. Jest tylko przerzucenie na sektor prywatny, natomiast cyberhigiena, zwłaszcza w instytucjach publicznych, jest jeszcze ważniejsza niż hardware czy software. Dlatego że, każdy haker to powie, on nie musi mieć łatwego systemu do włamania. On musi mieć po drugiej stronie osobę niekompetentną, nieprzeszkoloną, której on wykradnie hasło i wejdzie na jej login. Dziękuję bardzo.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję uprzejmie. Bardzo proszę, pani i pan dyrektor.

Specjalista do spraw legislacji w Polskim Towarzystwie Gospodarczym Sonia Kurpiel:

Szanowni państwo, Sonia Kurpiel, Polskie Towarzystwo Gospodarcze. Obawiamy się, że projekt ustawy będzie stanowił nadregulację. W praktyce uznanie dostawcy za dostawcę wysokiego ryzyka pozwoli na administracyjne wykluczenie firm z rynku. Przedsiębiorcy zostaną zmuszeni do ponoszenia znacznych kosztów bez wsparcia i bez oceny proporcjonalności. I właśnie to chcemy podkreślić jako strona biznesowa. Dziękuję.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Bardzo dziękuję. Proszę, panie dyrektorze.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa MC Marcin Wysocki:

Dziękuję. Panie przewodniczący, Wysoka Komisjo, zaiste warto słuchać Mario Draghiego, który wskazuje w swojej ocenie niestety taką przykrą konstatację, że... Przetłumaczę na język polski, raport jest w języku angielskim. W 2023 w raporcie z implementacji Toolbox 5G było napisane, że 14 krajów członkowskich nie miało wprowadzonych właśnie środków dotyczących dostawcy wysokiego ryzyka oraz innych kluczowych środków.

W tym samym czasie Chiny ograniczyły eksport dla dwóch wendorów dostawców sprzętu telekomunikacyjnego. Nie wszystkie kraje przyjęły środki do ochrony obywateli Europy, Europejczyków, ich danych osobowych, sieci telekomunikacyjnych w Unii oraz nie zapewniły wsparcia dla dostawców europejskich od praktyk nierynkowych, praktyk antykonkurencyjnych ze strony podmiotów z państw trzecich, wendorów dostawców. Czyli mamy taką sytuację, w której my nie wspieramy polskich i europejskich przedsiębiorców, tylko jesteśmy otwarci na różne antykonkurencyjne, dyskryminujące praktyki ze strony dostawców pochodzących z państw trzecich i Mario Draghi wskazuje to jako bardzo, bardzo istotny problem.

Co do tej kwestii było kilka krajów, w większości krajów, tak jak wskazywałem, Toolbox 5G już jest wdrożony, również w Rumunii jest wdrożony, już nawet czynności związane z wdrożeniem, czyli jakby te akty stosowania prawa zostały przyjęte. Natomiast co do tej wypowiedzi sprzed chwili, to oczywiście ta procedura jest tak zaplanowana, żeby te środki były proporcjonalne, dlatego te analizy są tak szczegółowe, zawierają aspekty techniczne i nietechniczne.

Natomiast wracając jeszcze do wypowiedzi mojego przedmówcy co do bezpieczeństwa łańcucha dostaw i dostawców wysokiego ryzyka, to fakt, że w przypadku badania bezpieczeństwa łańcucha dostaw to ktoś może być niebezpieczny, bo jest na przykład jedynym dostawcą. To instytucja dostawcy wysokiego ryzyka skupia się na innym czynniku, na takim założeniu, że te ryzyka, które są związane z dostarczaniem danego sprzętu, są zbyt wysokie, są nieakceptowalne, że nie można podjąć innych działań mitygujących. Natomiast ten dostawca ryzyka mieści się w takiej identyfikacji dostawcy wysokiego ryzyka w ramach bezpieczeństwa łańcucha dostaw, choć to pojęcie szersze i na pewno wszyscy eksperci, którzy specjalizują się w tej tematyce, wiedzą. Dziękuję, panie przewodniczący.

Przewodniczący poseł Bartłomiej Pejo (Konfederacja):

Dziękuję uprzejmie. Czy jeszcze ktoś z państwa chciałby zabrać głos w tym punkcie w tej dyskusji? Nie widzę, w takim razie bardzo serdecznie dziękuję za tę dyskusję. Myślę, że mimo wszystko i czasami pomimo braku merytoryki ta dyskusja była potrzebna. Myślę, że trzeba będzie wrócić jeszcze niejednokrotnie do tego tematu. Oczywiście oczekujemy na procedowanie ze strony ministerstwa.

Drody państwo, zamykam dyskusję. Bardzo serdecznie dziękuję za dzisiejsze posiedzenie.