Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Warszawa, dn. 02.02.2021 r.
KIGEiT/365/02/2021

Szanowny Pan Mateusz Morawiecki
Prezes Rady Ministrów
Minister Cyfryzacji
Kancelaria Prezesa Rady Ministrów

Szanowny Panie Premierze,

W dniu 22 stycznia 2021 na stronie internetowej Rządowego Centrum Legislacji zostały zamieszczone wyniki opiniowania, uzgodnień oraz konsultacji publicznych projektu Ustawy o zmianie Ustawy o krajowym systemie cyberbezpieczeństwa oraz Ustawy – Prawo zamówień publicznych. Jednocześnie projekt pod zmienioną nazwą został skierowany do prac Komitetów Rady Ministrów i kolejnych etapów procesu legislacyjnego pomimo obszernej tabeli nieuwzględnionych uwag i rozbieżności oraz dodania kluczowych, niekonsultowanych zapisów. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji (dalej „***Izba***" lub „***KIGEiT***") stanowczo sprzeciwia się takiemu trybowi prac nad projektem Ustawy oraz pragnie wyrazić w poniższym stanowisku opinię w stosunku do wersji projektu opatrzonej datą 20 stycznia 2021 r. oraz dostępnych już uwag zgłoszonych w ramach prac Komitetu ds. Cyfryzacji.

W art. 1 ust 2 pkt 1 projektu ustawy znajduje się informacja, iż do przedsiębiorców telekomunikacyjnych nie stosuje się zawartych w ustawie przepisów dotyczących bezpieczeństwa i zgłaszania incydentów za wyjątkiem art. 66a-66c, art. 67a-67b i art. 73 -74. Nie został dokładnie wyjaśniony zakres pozostałych przepisów, niedotyczących bezpieczeństwa i zgłaszania incydentów, które miałyby dotyczyć przedsiębiorców telekomunikacyjnych. Powyższe wyłączenie jest spełnieniem części postulatów zgłaszanych w trakcie konsultacji publicznych przez szereg podmiotów reprezentujących branżę telekomunikacyjną. Przedsiębiorcy telekomunikacyjni nie zostaną więc podmiotami Krajowego Systemu Cyberbezpieczeństwa w rozumieniu ustawy, do czego kwalifikowały je proponowane we wcześniejszej wersji projektu zapisy. Z przepisów zawartych w nowym projekcie wynika jednak, że niektóre z nich, dotyczące np. oceny dostawców sprzętu i oprogramowania, ostrzeżeń i poleceń zabezpieczających, mogą obejmować przedsiębiorców telekomunikacyjnych oraz być sankcjonowane karami finansowymi i właściwie zobowiązują przedsiębiorców telekomunikacyjnych do uczestnictwa w systemie.

1. **Art. 66 a ust. 1 zakres podmiotów objętych postępowaniem w sprawie uznania za dostawcę wysokiego ryzyka**

Izba z aprobatą przyjmuje ograniczenie zakresu podmiotowego obowiązku wycofania sprzętu lub oprogramowania od dostawcy uznanego za dostawcę wysokiego ryzyka i objęcie nim jedynie tych spośród przedsiębiorców telekomunikacyjnych, którzy są obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a PT.

Niemniej jednak należy podkreślić, że objęcie taką oceną dostawców sprzętu lub oprogramowania wykorzystywanych przez przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń wydaje się być zbyt daleko idącym środkiem, znacznie wykraczającym poza zasadę proporcjonalności. Dlatego naszym zdaniem, uwzględniając wagę proponowanych rozwiązań cyberbezpieczeństwa Rzeczypospolitej Polskiej, zasadne wydaje się zaadresowanie postępowania w sprawie oceny dostawcy wysokiego ryzyka do pomiotów, których produkty i usługi będą wykorzystywane przez operatora sieci komunikacji strategicznej (OSKS). Zgodnie z art. 59zd ust. 1-2 Projektu, sieć komunikacji strategicznej będzie zarządzana przez spółkę Skarbu Państwa, będącą przedsiębiorcą telekomunikacyjnym, posiadającą infrastrukturę telekomunikacyjną, która służyć będzie realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji. Z kolei przepis art. 59zd ust. 4 Projektu wymienia kluczowe urzędy i organy dla funkcjonowania państwa i bezpieczeństwa narodowego (przepis art. 59zd ust. 4 pkt 5 Projektu wymienia wprost Biuro Bezpieczeństwa Narodowego). OSKS świadczy usługi telekomunikacyjne w celu realizacji zadań w zakresie obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego na rzecz kluczowych dla bezpieczeństwa państwa urzędów i organów (art. 59zd ust. 3 Projektu). W sposób oczywisty podstawową kwestią jest więc zapewnienie bezpieczeństwa świadczonych usług telekomunikacyjnych przez OSKS. Kluczowym elementem tego procesu musi być funkcjonujący mechanizm weryfikacji podmiotów dostarczających produkty i usługi ICT dla OSKS. Wprost wynika to także z postanowień Projektu dotyczących oceny dostawców produktów i usług ICT (art. 66a ust. 6 pkt 1 Projektu przewiduje obowiązek dla Kolegium dokonania oceny zagrożenia bezpieczeństwa narodowego). Wskazane już zostało, że musi być zagwarantowane bezpieczeństwo świadczonych usług przez OSKS z punktu widzenia bezpieczeństwa narodowego. W związku z tym, jeżeli wymagane jest zapewnienie bezpieczeństwa świadczonych usług telekomunikacyjnych przez OSKS, to niezbędnym jest także zweryfikowanie dostawców usług i produktów ICT, koniecznych do świadczenia przez OSKS usług telekomunikacyjnych. Zweryfikowanie dostawców jest zapewniane właśnie przez mechanizm oceny dostawców przewidziany w art. 66a i następnych Projektu, który to mechanizm powinien być zastosowany także dla dostawców produktów i usług dla OSKS. Należy podkreślić, że przedstawione rozwiązanie nie tylko umożliwi zabezpieczenie podstawowych interesów Rzeczypospolitej w dziedzinie cyberbezpieczeństwa, ale również będzie środkiem proporcjonalnym z perspektywy krajowego oraz unijnego porządku prawnego.

2. Art. 66b ust. 1 pkt 2 – obowiązek wycofania sprzętu i oprogramowania

Jednocześnie Izba nadal wskazuje na potrzebę wydłużenia terminu wycofania sprzętu lub oprogramowania także w odniesieniu do przez przedsiębiorców telekomunikacyjnych objętych obowiązkiem.

W uzasadnieniu projektu wskazano: „*Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W proponowanych przepisach jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia."* Tzw. cykl życia urządzeń został więc teoretycznie uwzględniony w zmienionej wersji projektu. Jednak w odniesieniu do przedsiębiorców telekomunikacyjnych objętych obowiązkiem w praktyce utrzymany został termin 5 lat. W tym bowiem terminie winny zostać wycofane „*typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy"*. Przy tym z uwagi na konstrukcję wykazu (tj. określenie w nim kategorii funkcji) i jego bardzo

szeroki i ogólny zakres, w praktyce zachodzi ryzyko uznania każdego typu produktów ICT, rodzaju usług ICT i procesu ICT za objęty wykazem.

W ocenie Izby, nie jest uzasadnione, aby przedsiębiorców telekomunikacyjnych obowiązywał krótszy termin na wycofanie sprzętu lub oprogramowania niż średni cykl życia i czas amortyzacji urządzeń – tj. 7 lat. Nie jest również zasadne wyznaczenie dla przedsiębiorców telekomunikacyjnych okresu znacząco krótszego niż ustalony dla podmiotów krajowego systemu cyberbezpieczeństwa, właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej i przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym.

W tym kontekście nieadekwatne jest również stanowisko przedstawione w odniesieniu do zgłoszonych uwag: „*W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka."* Uznano, że wyznaczenie terminu odpowiadającego średniemu okresowi użytkowania sprzętu ma wykluczać rekompensaty, co jednak w żadnym razie nie uzasadnia odstąpienia od rekompensat w sytuacji wyznaczenia terminu o 30% krótszego.

Istotne znaczenie mają również kwestie związane z utrzymaniem sprzętu w czasie przed upływem terminu jego wycofania. W ocenie Izby, zachodzi potrzeba doprecyzowania projektowanych przepisów tak, aby nie zachodziły wątpliwości co do dopuszczalności działań utrzymaniowych polegających na stosownych wymianach czy modernizacjach sprzętu. W pewnych sytuacjach może nie być możliwa wymiana uszkodzonego lub niedziałającego sprzętu na dokładnie taki sam – np. w przypadku starszych urządzeń może zaistnieć konieczność zastąpienia go urządzeniem nowszej generacji lub posiadającym również dodatkowe funkcje, które potencjalnie może zostać zakwalifikowane jako należące do innego typu, w tym typu produktów określonego w decyzji, o której mowa w projektowanym art. 66a ust. 8.

W zakresie wymiany i modernizacji sprzętu nie powinno zachodzić ryzyko zakwalifikowania jej jako wprowadzania do użytkowania sprzętu danego typu w zakresie objętym decyzją – nie tylko w sytuacji wymiany urządzeń należących do tego samego, wycofywanego, typu określonego w decyzji, ale również w przypadku zastępowania urządzeń sprzętami należącymi do określonego w decyzji typu, który nie był wcześniej użytkowany przez dany podmiot, jeśli taka wymiana jest uzasadniona ze względów technicznych. Konieczność całkowitego wycofania sprzętu spowoduje, że w wyznaczonym w tym celu okresie przedsiębiorcy telekomunikacyjni będą ograniczać się do dokonywania jedynie niezbędnych zakupów sprzętu, gdyż dodatkowe inwestycje nie będą uzasadnione ekonomicznie. Wprowadzane przepisy nie powinny natomiast stać na przeszkodzie utrzymaniu sprzętu i zapewnieniu prawidłowego funkcjonowania sieci.

Przewidziane w projekcie ustawy uprawnienie ministra właściwego ds. informatyzacji do wydawania decyzji uznającej określonego dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka umożliwi wyeliminowanie części z nich. O ile proponowany przepis art. 66a ust. 3 określa KPA jako podstawę prawną postępowania w stosunku do adresata decyzji, to niezupełnie jasne jest czy podmiot nie będący adresatem a korzystający z produktów, usług, procesów dostarczonych przez adresata decyzji będzie mógł na tej podstawie wnieść swój sprzeciw lub skargę w przypadku uznania tego produktu, usługi czy procesu za wysoce ryzykowne.

Wynikający z art. 66b obowiązek wycofania z użytkowania określonych w decyzji produktów, usług czy procesów w ciągu 5 lat, przez podmioty zobowiązane do posiadania planów działań w sytuacjach szczególnych zagrożeń oraz pod warunkiem ich umieszczenia na liście

stanowiącej załącznik nr 3 do Ustawy jest zbyt krótkim terminem z uwagi na cykl życia produktu. Należy zaznaczyć, iż podmioty, dla których przewidziano tak krótki termin wycofania są dużo większe od tych którym umożliwiono wydłużenie tego okresu do 7 lat. Co za tym idzie będą one posiadać wielokrotnie wyższą liczbę urządzeń kwalifikujących się do wymiany co wymaga dłuższego czasu. Ponadto, brak możliwości otrzymania rekompensat z tytułu nałożonego obowiązku wycofania produktów oznacza kolejne, wynikające z przepisów ustawy straty finansowe dla przedsiębiorców telekomunikacyjnych.

3. Niejasna przesłanka „bezpieczeństwa narodowego" dla decyzji o dostawcy wysokiego ryzyka

Kluczowe dla oceny dostawcy określenie „bezpieczeństwo narodowe" nie posiada definicji legalnej, w szczególności nie jest zdefiniowane w k.s.c.u. W uzasadnieniu (s. 82), Projektodawcy powołują się na poglądy doktryny odnośnie definicji „bezpieczeństwa narodowego". Poglądy doktryny nie są jednak jednolite. Będzie to rodzić liczne wątpliwości interpretacyjne dotyczące określenia co to jest bezpieczeństwo narodowe i kiedy jest poważnie zagrożone. Projekt powinien się odnosić w tych kwestiach do pojęć posiadających definicje legalne.

Tymczasem „bezpieczeństwo narodowe" jest pojęciem traktatowym. Prawo UE w sposób wyraźny wyłącza kwestie związane z bezpieczeństwem narodowym z kompetencji organów unijnych. Bezpieczeństwo narodowe jest wyłączną prerogatywą państw członkowskich. Regulacja, której dotyczy Projekt, stanowi swego rodzaju implementację podejścia unijnego – w szczególności ma na celu urzeczywistnienie zasad, o których mowa w dokumencie 5G Toolbox. Jak zaś wskazano, regulacja unijna nie może – w świetle Traktatów – odnosić się do kwestii bezpieczeństwa narodowego. Z tego względu posłużenie się tym pojęciem w Projekcie (i znowelizowanej ustawie) będzie obarczone istotnym błędem systemowym i może prowadzić do dużych wątpliwości co do prawidłowego sposobu jego wykładni.

4. Kryteria oceny dostawcy

Projekt ustawy w art. 66a ust.1, ponownie koncentruje się na podmiotowej ocenie dostawcy produktów lub usług ICT, zamiast na ocenie tych produktów lub usług. W art. 66a ust. 6 wśród kryteriów oceny nadal też wymienia kryteria pozwalające na uznaniową ocenę, jak stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i danym państwem, czy zdolność ingerencji państwa, w którym ma siedzibę dostawca, w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Tymczasem, ocena musi być dokonywana w oparciu o precyzyjnie określone, jasne, niebudzące wątpliwości i weryfikowalne kryteria.

Postanowienia Projektu w zakresie dodania art. 66a ust. 6 pkt 2 lit. a-d, określające kryteria przeprowadzania oceny, należy uznać za sprzeczne z przepisami § 6 Rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz.U. Nr 100, poz. 908 ze zm.), zgodnie z którym, przepisy ustawy powinny być tak zredagowane, aby dokładnie i w sposób zrozumiały dla adresatów zawartych w nich norm wyrażały intencje prawodawcy. Wbrew komentarzom Projektodawców do uwag z konsultacji publicznych, kryteria oceny nie opierają się na kryteriach technicznych, gdyż ilość i rodzaj tych kryteriów (art. 66a ust. 6 pkt 4-6 Projektu), jest bardzo ograniczona. Nie tworzą one systemowych i spójnych rozwiązań. Trudno zrozumieć, dlaczego do kryteriów o charakterze technicznym nie dodano przynajmniej certyfikacji sprzętu i funkcji krytycznych, skoro został dodany do projektu ustawy cały rozdział 11a poświęcony właśnie certyfikacji cyberbezpieczeństwa.

5. Zakres decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka

Projekt ustawy przewiduje, że postępowanie będzie odnosić się do dowolnego dostawcy, z którego produktów, usług lub procesów korzystają podmioty wymienione w ustawie, o ile stwierdzona zostanie przesłanka poważnego zagrożenia dla bezpieczeństwa narodowego.

Tymczasem zgodność z podejściem europejskim (5G Toolbox) jak i zakładanymi celami regulacji nakazuje przyjąć, że ocena powinna odnosić się sprzętu i oprogramowania który realizuje funkcje krytyczne.

Ponadto decyzja ministra właściwego do spraw informatyzacji powoduje nie tylko pośrednio nakaz niewprowadzania przez danego dostawcę sprzętu, oprogramowania oraz usług określonych w tej decyzji, ale także bezpośredni zakaz wprowadzania do używania takiego sprzętu, oprogramowania i usług skierowany wobec innych podmiotów krajowego systemu cyberbezpieczeństwa, w tym przedsiębiorców telekomunikacyjnych. Zakres oddziaływania decyzji jest więc niezmiernie szeroki, jednak skutki decyzji dla podmiotów, na których oddziałuje, nie zostały dostatecznie przeanalizowane (choćby w zakresie możliwości rekompensaty, możliwości wzruszenia decyzji itp.) – co wynika z uzasadnienia projektu i udostępnionej OSR.

6. Nieprawidłowe odstępstwa dotyczące procedury administracyjnej

W projekcie ustawy przewidziano cały szereg odstępstw od kardynalnych zasad nie tylko procedury administracyjnej, ale każdego rzetelnego postępowania: decyzja w sprawie oceny dostawcy nie będzie musiała być uzasadniona (art. 66a ust. 10); sąd będzie rozpoznawał sprawę na posiedzeniu niejawnym (art. 66d ust. 1); skarżący podmiot nie otrzyma pełnego uzasadnienia wyroku (art. 66d ust. 2). Ponadto decyzja będzie podlegała natychmiastowemu wykonaniu (art. 66a ust. 12), a nawet sąd nie będzie mógł wstrzymać jej wykonania, choćby to groziło nieodwracalnymi skutkami (art. 66d ust. 3). W ten sposób postępowanie to będzie spełniało cechy procesu inkwizycyjnego. Wbrew twierdzeniom w uzasadnieniu projektu ustawy, że „*strona i tak będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym*", nie będzie jednak w praktyce miała dostępu do dowodów i materiałów postępowania, skoro niejawne będzie posiedzenie i uzasadnienie wyroku. W sposób więc oczywisty jej prawa w tym postępowaniu zostaną ograniczone. Wbrew także twierdzeniom Projektodawców w uzasadnieniu, że w „*zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców*", z uwagi na rygor natychmiastowej wykonalności decyzji w sprawie dostawcy wysokiego ryzyka, połączony z zakazem dla sądu wstrzymania wykonania wykonalności decyzji, taki mechanizm oczywiście będzie istniał.

Możliwość wstrzymania wykonania zaskarżonej decyzji administracyjnej przez sąd, stanowi środek tzw. ochrony tymczasowej w postępowaniu sądowoadministracyjnym. Ochrona tymczasowa jest przy tym niezbędna do realizacji efektywnej ochrony sądowej, stanowiącej jeden z fundamentów zasady prawa do sądu wyrażonej nie tylko w Konstytucji, ale także w Karcie Praw Podstawowych UE oraz Europejskiej Konwencji Praw Człowieka. Brak zapewnienia środków ochrony tymczasowej – a więc brak możliwości zapobieżenia nieodwracalnym skutkom wadliwych aktów administracyjnych – skutkuje tym, że ochrona sądowa staje się jedynie pozorna i nie realizuje swoich funkcji. Mimo późniejszego uchylenia wadliwego aktu administracyjnego strona i tak ponosi nieodwracalne konsekwencje jego wydania.

Wynikający z art. 66b obowiązek wycofania z użytkowania określonych w decyzji produktów, usług czy procesów w ciągu 5 lat, przez podmioty zobowiązane do posiadania planów działań w sytuacjach szczególnych zagrożeń oraz pod warunkiem ich umieszczenia na liście stanowiącej załącznik nr 3 do Ustawy jest zbyt krótkim terminem z uwagi na cykl życia

produktu. Należy zaznaczyć, iż podmioty, dla których przewidziano tak krótki termin wycofania są dużo większe od tych którym umożliwiono wydłużenie tego okresu do 7 lat. Co za tym idzie będą one posiadać wielokrotnie wyższą liczbę urządzeń kwalifikujących się do wymiany co wymaga dłuższego czasu. Ponadto, brak możliwości otrzymania rekompensat z tytułu nałożonego obowiązku wycofania produktów oznacza kolejne, wynikające z przepisów ustawy straty finansowe dla przedsiębiorców telekomunikacyjnych.

7. Art. 73 ust. 2a – kary finansowe

Izba pragnie wyrazić sprzeciw wobec nakładania na przedsiębiorców telekomunikacyjnych kar finansowych za naruszenie obowiązków niewynikających ani z przepisów rangi ustawowej, ani z decyzji administracyjnej, której dany przedsiębiorca jest adresatem.

W projektowanym art. 73 ust. 2a karą pieniężną zagrożone zostało niedostosowanie się przez dany podmiot do obowiązków określonych w art. 66b. Przy tym obowiązki te są „nakładane" na dany podmiot w formie opublikowanej informacji o decyzji wydanej wobec innego podmiotu (dostawcy), w postępowaniu administracyjnym, którego podmiot obowiązany nie był stroną.

Co więcej, spośród obowiązków określonych w projektowanym art. 66b jedynie obowiązkowi, o którym mowa w ust. 1 pkt 2 zostały wyznaczone konkretne ramy czasowe – tj. „*7 lat od dnia opublikowania informacji o decyzji, o której mowa w art. 66a ust. 8*", podczas gdy w przypadku obowiązku z ust. 2 ujęto określenie „*w ciągu 5 lat*", jednak bez wskazania, od jakiego momentu powyższe 5 lat ma być liczone, a w przypadku obowiązków z ust. 1 pkt 1 oraz ust. 3 w ogóle zaniechano określenia momentu, od jakiego ma następować niewprowadzanie do użytkowania oraz niedokonywanie zamówień sprzętu, oprogramowania i usług.

Przyjęcie, że – podobnie jak w ust. 1 pkt 2 – również pozostałe obowiązki miałyby ciążyć na podmiotach od opublikowania informacji o decyzji prowadziłoby do sytuacji, w której nałożenie kary mogłoby nastąpić za działania podjęte przez przedsiębiorcę telekomunikacyjnego jeszcze przed formalnym uznaniem dostawcy za dostawcę wysokiego ryzyka, tj. przed związaniem decyzją jej adresata, czyli przed doręczeniem decyzji, a w przypadku publicznego obwieszczenia przez udostępnienie pisma w Biuletynie Informacji Publicznej na stronie podmiotowej właściwego organu administracji publicznej – przed upływem czternastu dni od dnia, w którym nastąpiło publiczne obwieszczenie (art. 49 § 2 KPA).

8. Art. 59zd – Operator Sieci Komunikacji Strategicznej

Projekt został wzbogacony o rozdział 11b dający możliwość powołania spółki skarbu państwa będącej operatorem sieci komunikacji strategicznej (dalej: „OSKS"). Zasoby (w tym elementy sieci telekomunikacyjnej) za pomocą których operator ma świadczyć usługi na potrzeby podmiotów wymienionych w art. 59zd ust. 4 oraz innych (ust. 5), mają pochodzić również od posiadających je operatorów sieci. Wprowadzenie OSKS na rynek oraz wyłączenie z grona klientów podmiotów publicznych korzystających obecnie na zasadach komercyjnych z usług telekomunikacyjnych zaburza konkurencję na rynku usług telekomunikacyjnych oraz prowadzi do gwałtownego uszczuplenia przychodów w perspektywie kolejnych lat. Wejście na rynek telekomunikacyjny podmiotu, który miałby świadczyć usługi dla podmiotów wymienionych we wskazanych artykułach oznacza faktyczną nacjonalizację rynku public. Straty z tego tytułu spowodują, że niektóre podmioty, wyspecjalizowane w dostarczaniu usług na najwyższym poziomie, stracą możliwość odzyskania środków dokonanych w ramach inwestycji oraz będą wymagały zmiany strategii. Umożliwienie stworzenia OSKS i przejęcia przez niego części rynku telekomunikacyjnego było spodziewane i zapowiadane od wielu lat. Zamiar taki spotykał się zazwyczaj ze sprzeciwem nie tylko branży telekomunikacyjnej ale również przedstawicieli

administracji. Włączenie zapisów tak istotnych dla rynku i jego uczestników, mających wpływ na jego konkurencyjność oraz swobodę działalności gospodarczej w sposób niezgodny z regułami transparentności czy rzetelności będzie stanowić dużą przeszkodę w trakcie dalszych prac oraz ewentualnej implementacji przepisów w tak istotnej dziedzinie jak cyberbezpieczeństwo.

Łatwo odnieść wrażenie, że proces konsultacji został potraktowany jako formalny obowiązek, którego realizacja miała służyć akceptacji zapisów, które zostały dodane po ich zakończeniu.

Z przedstawionych przez Ministerstwo Aktywów Państwowych uwag do projektu ustawy w ramach prac w Komitecie ds. Cyfryzacji wynika, że OSKS miałby korzystać z wielu udogodnień, posiadać szereg uprawnień oraz pozycję jakiej żaden inny podmiot nie jest w stanie osiągnąć bez pomocy ze strony Państwa. Zaproponowany zakres obligatoryjnych zadań jakie ma wykonywać OSKS dla MON, MSWiA i MSZ a także budowa i utrzymanie Bezprzewodowej Sieci Łączności Specjalnej (BSŁS) powoduje, że funkcjonowanie podmiotów świadczących aktualnie usługi dla wymienionych Ministerstw i podległych im jednostek, a także aukcja pasma pod budowę sieci 5G wydają się zagrożone. Spodziewana kwota przychodu z aukcji 5G z pewnością powinna zostać zrewidowana ponieważ świadczenie usług na okrojonym rynku przyniesie zwycięzcom aukcji mniejszy przychód.

OSKS miałby świadczyć również usługi wsparcia technicznego, a także inne usługi nie wymienione w ustawie o ile uprawnione podmioty tego zażądają.

OSKS miałby być również uprawniony do bezpłatnego umieszczania obiektów i urządzeń infrastruktury telekomunikacyjnej (urządzeń i kabli) na nieruchomościach Skarbu Państwa, Lasów Państwowych, państwowych osób prawnych, jednostek samorządu terytorialnego oraz państwowych lub samorządowych jednostek organizacyjnych. Ponadto wyłączone miałoby zostać stosowanie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2019 r. poz. 2019 i z 2020 r. poz. 288, 1517 oraz 2320) w stosunku do umów zawieranych przez OSKS w celu realizacji jego zadań.

9. Art. 59zf – wprowadzenie regulacji w zakresie dostępu do sieci telekomunikacyjnej

Izba pragnie stanowczo zakwestionować projektowany obowiązek zapewniania dostępu do elementów sieci telekomunikacyjnej na potrzeby komunikacji strategicznej realizowanej przez operatora sieci komunikacji strategicznej.

W pierwszej kolejności należy wskazać, że nie jest jasne, na jakie podmioty obowiązek taki ma zostać nałożony. W projektowanym przepisie mowa bowiem o „operatorze telekomunikacyjnym". Należy zwrócić uwagę, że jest to pojęcie odmienne od pojęcia operatora, zdefiniowanego w art. 2 pkt 27 lit. b) ustawy Prawo telekomunikacyjne oraz w projektowanym art. 2 pkt 42 lit. b) ustawy Prawo komunikacji elektronicznej. Co więcej, każdy „operator" w rozumieniu PT i PKE jest przedsiębiorcą telekomunikacyjnym, natomiast do przedsiębiorców telekomunikacyjnych ustawy o Krajowym systemie bezpieczeństwa nie stosuje się i, zgodnie z projektowanym art. 1 ust. 2 pkt 1, ma tak pozostać, z wyjątkiem wyraźnie wskazanych przepisów, tj. art. 66a-66c, art. 67a-67b i art. 73-74. W uzasadnieniu projektu wskazano wyraźnie, że *„[d]o przedsiębiorców telekomunikacyjnych będą się stosować:*

1) *przepisy o wycofaniu produktów ICT, usług ICT, procesów ICT pochodzących od dostawcy wysokiego ryzyka*
2) *przepisy o ostrzeżeniu i poleceniu zabezpieczającym*
3) *przepisy o karach pieniężnych."*

Choć przedmiot projektowanego przepisu, jak również właściwość Prezesa UKE, wskazują na taką intencję, podmiotem obowiązku przewidzianego w projektowanym art. 59zf nie może być więc operator – będący przedsiębiorcą telekomunikacyjnym.

Następnie należy zakwestionować bezwzględny charakter projektowanego obowiązku. Obowiązek ten, nakładany na rynku niepodlegającym regulacji *ex ante*, będzie umożliwiać żądanie zapewnienia nieograniczonego dostępu do wszystkich elementów sieci telekomunikacyjnej każdego „operatora telekomunikacyjnego".

W projektowanym przepisie zaznaczono wymóg odpłatności dostępu, lecz nie zostały wskazane jakiekolwiek kryteria, w oparciu o które następowałoby wyznaczenie poziomu opłat. W praktyce oznacza to ryzyko narzucenia w ramach decyzji opłat za świadczony dostęp nie tylko na poziomie nierynkowym, ale również znacząco poniżej kosztów, a wręcz za symboliczną „złotówkę".

Zobowiązanie „operatorów telekomunikacyjnych" do zapewnienia warunków oraz finansowania działalności operatora sieci komunikacji strategicznej, który jednocześnie będzie uprawniony do komercyjnego świadczenia usług telekomunikacyjnych na rzecz potencjalnie nieograniczonego zakresu podmiotów (za zgodą Prezesa Rady Ministrów), stanowi rażąco nadmierną ingerencję w prowadzoną przez „operatorów telekomunikacyjnych" działalność gospodarczą.

10. Art. 115^4 ustawy Prawo telekomunikacyjne – przyznanie częstotliwości z naruszeniem wymogów dotyczących procedury selekcyjnej

W uzasadnieniu projektu nowelizacji wskazano, że „*Zmiana zaproponowana w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne ma na celu zapewnienie odpowiednich mechanizmów Prezesowi UKE, które mogą w przyszłości doprowadzić do zintensyfikowania działań mających na celu realizację przez Rzeczpospolitą Polską celów w zakresie zapewnienia dostępu do usług szerokopasmowych każdemu obywatelowi Unii Europejskiej."* oraz powołano się na ambitne cele wynikające z unijnych dokumentów programowych. Trudno jednak dopatrzeć się związku pomiędzy projektowanym wprowadzeniem procedury jawnie sprzecznej z unijnymi wymogami przyznawania praw użytkowania widma radiowego a przywołanymi celami.

W dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (dalej: „EKŁE") wyraźnie wskazano, że przyznawanie praw do użytkowania częstotliwości następuje według kryteriów selekcji i procedury selekcyjnej, które muszą być obiektywne, przejrzyste, niedyskryminacyjne oraz proporcjonalne (art. 55 ust. 6). Analogiczny wymóg przewidziany był również w poprzedzającej EKŁE dyrektywie 2002/20/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (dyrektywa o zezwoleniach).

Tymczasem projektowany przepis zupełnie pomija powyższe wymogi, a nawet przewiduje całkowite odstąpienie od procedury selekcji na rzecz arbitralnego „wyznaczenia" dysponenta częstotliwości przez Prezesa Rady Ministrów.

Projekt przepisu art. 115^4 ustawy Prawo telekomunikacyjne należy stanowczo zakwestionować – zarówno jako jawne pogwałcenie określonych w prawie unijnym wymogów dysponowania widmem, a także niezależności krajowego organu regulacyjnego, jak i z uwagi na sprzeczną z Konstytucją RP formę, jaką miałoby ono przybrać.

„Wyznaczanie" dysponenta częstotliwości przez Prezesa Rady Ministrów odbywałoby się bowiem „bez żadnego trybu", poza postępowaniem w sprawie dokonania rezerwacji częstotliwości, pozostając całkowicie dowolnym i niepodlegającym jakiejkolwiek kontroli instancyjnej czy sądowej. Nie zmienia tego faktu okoliczność, że już po „wyznaczeniu" dysponenta Prezes UKE wszczynałby i prowadził postępowanie w przedmiocie dokonania rezerwacji częstotliwości na rzecz uprzednio wybranego podmiotu.

Niedopuszczalne jest nie tylko narzucanie Prezesowi UKE rozstrzygnięcia faktycznie podjętego uprzednio przez Prezesa Rady Ministrów, ale również uzależnienie wydania decyzji rezerwacyjnej od zgody ministra właściwego do spraw informatyzacji. W art. 8 ust. 1 EKŁE wskazano wyraźnie, że krajowe organy regulacyjne działają niezależnie i nie występują o instrukcje do żadnego innego podmiotu ani nie przyjmują takich instrukcji w związku z wykonywaniem zadań przydzielonych im na podstawie prawa krajowego wdrażającego prawo Unii (analogiczny wymóg niezależności krajowych organów regulacyjnych ujęty był w art. 3 ust. 3a dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa).

Związanie Prezesa UKE stanowiskiem ministra jest wprost sprzeczne z powyższym przepisem. Przy tym istota współdziałania organów administracji polega na zasięganiu w ramach postępowania głównego stanowiska innego organu w zakresie jego właściwości – jak np. zasięganie przez Prezesa UKE opinii Prezesa UOKiK w sprawie zachowania warunków konkurencji czy opinii Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu dotyczącej okoliczności prowadzących do zagrożenia obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. W projektowanym zaś wymogu uzyskiwania stanowiska ministra właściwego do spraw informatyzacji – i to w formie wiążącej zgody – trudno dopatrzeć się jakiegokolwiek innego celu poza całkowitym podporządkowaniem rozstrzygnięć Prezesa UKE administracji rządowej. Po „wyznaczeniu" dysponenta częstotliwości przez Prezesa Rady Ministrów, Prezes UKE w toku postępowania rezerwacyjnego winien bowiem badać spełnienie przesłanek ustawowych dokonania rezerwacji, potencjalnie mogłaby więc zostać wydana decyzja niezgodna z dokonanym z góry wyborem dysponenta rezerwacji. Natomiast związanie Prezesa UKE stanowiskiem ministra właściwego do spraw informatyzacji pozwoli wykluczyć jakąkolwiek swobodę działania regulatora w tym zakresie, nadając jednocześnie rządowemu rozstrzygnięciu fasadową formę decyzji Prezesa UKE.

11. Art. 67a i art. 67b – ostrzeżenia Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

O ile projektowany w art. 67a system wydawania ostrzeżeń przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w zakresie cyberzagrożeń obejmuje akceptowalne formy wywierania presji, w formie zaleceń określonego sposobu postępowania w celu uniknięcia możliwości wystąpienia incydentu krytycznego, to możliwość wydawania poleceń zabezpieczających przez ministra właściwego ds. informatyzacji może prowadzić do nałożenia kary do 3% rocznego globalnego przychodu na podmiot działający wbrew nakazom wynikającym z polecenia zabezpieczającego. Jako pozytywną należy określić zmianę powodującą, że przepisy KPA będą miały zastosowanie do procedury wydawania poleceń zabezpieczających.

Krajowy system certyfikacji bezpieczeństwa, którego ramy i sposób funkcjonowania zostały opisane w rozdziale 11a projektu ustawy jest wprost oparty na wytycznych zawartych w Akcie o Cyberbezpieczeństwie tj. Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. Jednak, art. 59o daje ministrowi właściwemu do spraw informatyzacji prawo do zatwierdzenia lub odmowy zatwierdzenia certyfikatu odwołującego się do poziomu uzasadnienia „wysoki" co wydaje się działaniem podyktowanym wyłącznie politycznym motywem.

Pomimo szerokiego sprzeciwu branży telekomunikacyjnej spodziewane jest objęcie PT wymaganiami usuniętymi z projektu a pochodzącymi z poprzedniej iteracji projektu Ustawy o KSC, dotyczącymi obowiązków związanych ze zgłaszaniem incydentów do odpowiedniego

CSIRT oraz powołania CSIRT Telco. Działanie takie zostało zapowiedziane w odpowiedzi na zgłoszone w konsultacjach uwagi i zostanie zrealizowane w ustawie Prawo Komunikacji Elektronicznej oraz Ustawie wprowadzającej Ustawę Prawo Komunikacji Elektronicznej. Istotnym będzie porównanie tego zakresu obowiązków i faktyczne ustalenie czy przedsiębiorcy telekomunikacyjni nie będą podmiotami krajowego systemu cyberbezpieczeństwa ze względu na konieczność realizacji obowiązków dedykowanych ściśle sektorowi telekomunikacyjnemu, czy też będą podlegać dodatkowym wymaganiom i pomimo okrojenia potencjalnego zakresu działania związanego z przejęciem klientów przez OSKS zostaną zobligowani go rozbudowy systemów, zasobów i kompetencji w dziedzinie cyberbezpieczeństwa.

12. Wadliwa identyfikacja funkcji krytycznych sieci (Uwagi do Załącznika nr 3 do Projektu - wykaz funkcji krytycznych)

W sposób uznaniowy, bez odpowiedniej weryfikacji technicznej i rynkowej, zostały przedstawione w Załączniku nr 3 Kategorie funkcji krytycznych dla bezpieczeństwa sieci i usług. Tego rodzaju lista jest tworzona nie poprzez ogłoszenie w ustawie, ale jak pokazuje praktyka w innych krajach, np. Niemczech, jest przygotowywana przez regulatora rynku telekomunikacyjnego, we współpracy z organami odpowiedzialnymi za bezpieczeństwo. Następnie lista ta jest poddawana konsultacjom rynkowym, przedsiębiorcy telekomunikacyjni mogą zgłaszać do niej uwagi. Brak konsultacji z podmiotami zainteresowanymi skutkuje rozwiązaniem, które nie mają uzasadnienia w realnym poziomie ryzyka ani standardach międzynarodowych (przykładowo – uznanie za funkcję krytyczną elementów dostępowej infrastruktury radiowej sieci infrastruktury sieci komórkowych, tzw. RAN). Tymczasem unijny raport "*EU coordinated risk assessment of the cybersecurity of 5G networks*" oraz wytyczne "*Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*" do elementów krytycznych sieci zaliczają wyłącznie funkcje sieci rdzeniowej, tj. UDM, AUSF, SEPP, NRF, NEF, SMF, AMF oraz UPF., tj. RAN (Radio Access Network) nie należy do architektury sieci rdzeniowej i nie jest identyfikowana, jako element krytyczny sieci. Dodatkowo należy wskazać, iż rząd polski, w ramach analizy ryzyka wykonanej dla potrzeb opracowania raportu „Guidelines on common elements *for 5G cybersecurity risk assessments and structured template for reporting on findings*", odwołał się wyłącznie do funkcji sieciowych 5G. RAN nie został zidentyfikowany jako funkcja krytyczna.

Jednocześnie, zgodnie z prośbą otrzymaną w toku konsultacji wewnątrz-izbowych od jednego z członków Izby, firmy EXATEL S.A., informuję o wyłączeniu poparcia tej firmy dla treści powyższego stanowiska.

Wiceprezes Zarządu
Jarosław Tworóg

Prezes Zarządu
Stefan Kamiński

Do wiadomości:
Szanowny Pan Marek Zagórski - Sekretarz Stanu, Pełnomocnik ds. Cyberbezpieczeństwa, Kancelaria Prezesa Rady Ministrów