ZWIĄZEK TELEWIZJI KABLOWYCH W POLSCE IZBA GOSPODARCZA
90-113 ŁÓDŹ, UL. TRAUGUTTA 25
TELEFON: 606-368-161,
e-mail: ztk@ztkig.pl,
REGON: 471683422, NIP: 7251656807, KRS: 0000128771

L. dz. 04/01/25/PR

Kraków, 18.01.2025 r.

SZANOWNY PAN
PAWEŁ OLSZEWSKI
SEKRETARZ STANU W MINISTERSTWIE CYFRYZACJI

Szanowny Panie Ministrze

W imieniu Związku Telewizji Kablowych w Polsce Izba Gospodarcza, zwanej dalej ZTK, Izbą lub Izbą Gospodarczą, **która zrzesza wyłącznie mikro, małych i średnich przedsiębiorców z branży telekomunikacyjnej**, przedkładam uwagi krytyczne dotyczące propozycji wdrożenia do polskiego systemu prawnego instytucji dostawcy wysokiego ryzyka oraz instytucji polecenia zabezpieczającego, czemu nasza Izba Gospodarcza zdecydowanie się sprzeciwia wskazując w pierwszej kolejności na brak jakichkolwiek podstaw prawnych do wdrożenia w polskim systemie prawnych obu kwestionowanych przez nas instytucji.

Instytucja prawna decyzji uznania za dostawcę wysokiego ryzyka oraz procedura prowadząca do wydania decyzji o uznaniu za dostawcę wysokiego ryzyka

Wprowadzenie instytucji prawnej decyzji uznania za dostawcę wysokiego ryzyka polski projektodawca próbuje wdrożyć do polskiego systemu prawnego już po raz kolejny, tym razem czyniąc to w ramach projektu z dnia 23.04.2024 r. ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (nr w wykazie prac legislacyjnych i programowych Rady Ministrów UC32), zwanego dalej projektem ustawy zmieniającej ustawę o KSC.

Projektodawca do ustawy z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jedn. Dz. U. z 2024 r. poz. 1077 z późn. zm.), zwanej dalej ustawą o KSC, dodaje art. 67 b- art. 67 f poświęcone procedurze dotyczącej uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka (art. 1 pkt. 70 projektu ustawy zmieniającej ustawę o KSC).

Przede wszystkim wdrożenia przedmiotowej procedury i środków prawnych będących efektem jej wdrożenia do polskiego systemu prawnego nie można uznać za dążenie do zadośćuczynienia obowiązkowi implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148(dyrektywa NIS2)(Dz. U. U.E.L.2022.333.80), zwanej dalej Dyrektywą NIS 2,do wewnętrznego porządku prawnego naszego kraju.

Dyrektywa bowiem NIS 2 milczy na temat tego rodzaju środka prawnego, ani nie przewiduje jego wdrażania, ani tym bardziej w tym zakresie na państwa członkowskie nie nakłada obowiązku jego wdrożenia.

Oznacza to, iż wprowadzenie do wewnętrznego porządku prawnego przedmiotowej instytucji nie stanowi implementacji dyrektywy NIS 2, a zatem w omawianym przypadku nie mamy do czynienia z realizacją obowiązku prawnego wynikającego z normy art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej z dnia 25.03.1957 r. (Dz. U. z 2004 r. nr 90 poz. 864/2 z późn. zm.), zwanego dalej Traktatem o funkcjonowaniu Unii Europejskiej.

Natomiast prawodawca europejski przewiduje dla państw członkowskich uprawnienie, a nie obowiązek, wprowadzenia wobec podmiotów ważnych i podmiotów kluczowych wymogu stosowania konkretnych produktów ICT, usług ICT i procesów ICT opracowanych przez dany podmiot kluczowy lub ważny lub nabytych od osób trzecich certyfikowanych zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa (art. 24 ust. 1 zd. 1 dyrektywy NIS 2).
Ponadto prawodawca europejski dopuszcza opcję, iż państwa członkowskie będą zachęcały podmioty kluczowe i ważne do korzystania z kwalifikowanych usług zaufania (art. 24 ust. 1 zd. 2 dyrektywy NIS 2).

Niewątpliwie jednak regulacja art. 24 ust. 1 dyrektywy NIS 2 nie nakłada na państwa członkowskie obowiązku wdrożenia regulacji wewnętrznych obligujących podmioty kluczowe i ważne do nabywania od osób trzecich certyfikowanych produktów ICT, usług ICT i procesów ICT, a także certyfikowania opracowanych przez te podmioty (kluczowe i ważne) własnych produktów ICT, usług ICT i procesów ICT, a jedynie dopuszcza opcję, iż państwa członkowskie takie regulacje będą mogły w wewnętrznym porządku prawnym wdrażać.

Odnośnie z kolei kwalifikowanych usług zaufania regulacja art. 24 ust. 1 zd. 2 dyrektywy NIS 2 dopuszcza jedynie uprawnienie państw członkowskich do zachęcania podmiotów ważnych i kluczowych do korzystania z kwalifikowanych usług zaufania.

Natomiast w sytuacji stwierdzenia przez Komisję Europejską niewystarczających poziomów cyberbezpieczeństwa Komisja Europejska została wyposażona w możliwość przyjmowania aktów delegowanych w celu uzupełnienia dyrektywy NIS 2 poprzez określenie, od których kategorii podmiotów kluczowych i ważnych należy wymagać stosowania nabytych od osób trzecich certyfikowanych produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji dla swoich własnych produktów ICT, usług ICT i procesów ICT na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa (art. 24 ust. 2 dyrektywy NIS 2).
Jedynie zatem w takim wyjątkowym przypadku występowania niewystarczających poziomów cyberbezpieczeństwa w oparciu o aktywność normatywną Komisji Europejskiej (jeśli z niej skorzysta) zaistnieje obowiązek certyfikacji własnych produktów ICT, usług ICT i procesów ICT opracowanych przez podmioty ważne i kluczowe oraz powstanie obowiązek nabywania od osób trzecich przez podmioty kluczowe i ważne wyłącznie certyfikowanych na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT.

Ponadto państwa członkowskie w celu wspierania spójnego wdrażania dążenia do tego, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu nie narzucając, ani też nie faworyzując stosowania określonego rodzaju technologii zostały uprawnione do zachęcania podmiotów kluczowych i ważnych do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci systemów informatycznych (art. 25 ust. 1 dyrektywy NIS 2).
Także w tym przypadku państwa członkowskie nie zostały ani zobowiązane, ani też uprawnione do wdrożenia w wewnętrznym systemie prawnym regulacji przewidujących obowiązek stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych, a jedynie prawodawca europejski upoważnił je do stosowania systemów zachęt zmierzających do przekonania podmiotów kluczowych i ważnych do stosowania europejskich i międzynarodowych norm i specyfikacji technicznych istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych.

Powyższa analiza świadczy o tym, iż normalizacja dotycząca stosowania określonych rodzajów sieci i systemów informatycznych nie jest obowiązkowa w państwach członkowskich i państwa członkowskie nie zostały nawet uprawnione do narzucania w tym zakresie podmiotom kluczowym i ważnym normalizacji w tym zakresie (art. 25 ust. 1 dyrektywy NIS 2), natomiast certyfikacja nabywanych od osób trzecich przez podmioty kluczowe i ważne, jak i wytwarzanych przez podmioty kluczowe i ważne produktów ICT, usług ICT i procesów ICT co do zasady nie jest obligatoryjna w państwach członkowskich, zaś państwa członkowskie mogą, ale wcale nie muszą, w tym zakresie nałożyć stosowne obowiązki na podmioty ważne i kluczowe (at. 24 ust. 1 dyrektywy NIS 2), natomiast zupełnie wyjątkowo w razie stwierdzenia niewystarczających poziomów cyberbezpieczeństwa Komisja Europejska została wyposażona w uprawnienie do wydawanie aktów delegowanych, mocą których zostanie określone od których kategorii podmiotów kluczowych i ważnych należy wymagać stosowania nabytych od osób trzecich certyfikowanych produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji dla swoich własnych produktów ICT, usług ICT i procesów ICT opracowanych przez podmioty ważne i kluczowe na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa (art. 24 ust. 2 dyrektywy NIS 2).

W przypadku jednakże wydawania decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka nie mamy do czynienia ani z kwestią certyfikacji, ani też z kwestią normalizacji za nabywane od osób trzecich przez podmioty ważne i kluczowe produktów ICT, usług ICT i procesów ICT.

Tego rodzaju instytucji (decyzja i procedura prowadząca do jej wydania) dyrektywa NIS 2, ani też jakiekolwiek inne dyrektywy unijne lub decyzje unijne kierowane do konkretnych państw, w tym i do państwa polskiego, nie przewidują, a zatem nie zachodzi prawny obowiązek jej implementacji do wewnętrznego porządku prawnego naszego kraju (art. 288 zd. 4, zd., zd. 5, zd. 6 Traktatu o funkcjonowaniu Unii Europejskiej).

Analizując uzasadnienie projektu ustawy zmieniającej ustawę o KSC dochodzimy do wniosku, że projektodawca wywodzi potrzebę wprowadzenia instytucji uznania dostawcy za dostawcę wysokiego ryzyka z:

a/ zalecenia Komisji (UE) 2019/534 z dnia 26.03.2019 r. Cyberbezpieczeństwo sieci 5G (Dz.U. UE.L. 2019.88.42), zwanego dalej zaleceniem w sprawie Cyberbezpieczeństwa sieci 5G(str. 59-60 uzasadnienia projektu ustawy zmieniającej ustawę o KSC),

b/ Unijnej skoordynowanej oceny ryzyka cyberbezpieczeństwa sieci 5G, zwanej dalej Unijną oceną Cyberbezpieczeństwa sieci 5G(str. 61 uzasadnienia projektu ustawy zmieniającej ustawę o KSC),

c/ Unijnego zestawu środków dla sieci 5 G tzw. Toolbox 5G, zwanego dalej Toolbox 5G (str. 61 uzasadnienia projektu ustawy zmieniającej ustawę o KSC),

d/ Komunikatu Komisji Europejskiej z dnia 29.01.2020 r., zwanego dalej Komunikatem Komisji z 29.01.2020 r. (str. 62 uzasadnienia projektu ustawy zmieniającej ustawę o KSC).

Projektodawca zatem wprowadzenie instytucji decyzji uznania dostawcy za dostawcę wysokiego ryzyka, której wydanie stanowić będzie niewątpliwe ograniczenie konstytucyjnej wolności gospodarczej uzasadnia ważnym interesem publicznym [art. 22 Konstytucji Rzeczypospolitej Polskiej z dnia 2.04.1997 r. (Dz. U. nr 78 poz. 483 z późn. zm.), zwanej

dalej Konstytucją RP], który jednakże zostaje wywiedziony z zalecenia Komisji Europejskiej w sprawie Cyberbezpieczeństwa sieci 5G, które wolą prawodawcy unijnego nie posiada jakiejkolwiek mocy obowiązującej (art. 288 zd. 7 Traktatu o funkcjonowaniu Unii Europejskiej), a zarazem nie posiada waloru aktu prawnego powszechnie obowiązującego w ujęciu art. 87 Konstytucji RP, oraz z Unijnej oceny Cyberbezpieczeństwa sieci 5G, Toolbox 5G i Komunikatu Komisji z 29.01.2020 r., które to z kolei dokumenty(opracowania) nie stanowią ani źródła prawa Unii Europejskiej wskazanego w art. 288 zd. 1 Traktatu o funkcjonowaniu Unii Europejskiej, ani też źródła prawa powszechnie obowiązującego w ujęciu art.87 Konstytucji RP, co automatycznie przesądza o braku mocy wiążącej także tych trzech ostatnio wzmiankowanych dokumentów o charakterze nienormatywnym.

Wywiedzenie zatem ważnego interesu publicznego, który miałby przemawiać za ograniczaniem konstytucyjnej wolności gospodarczej poprzez wprowadzenie nowej instytucji do prawa polskiego (decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka) z trzech dokumentów o charakterze nienormatywnym nie posiadających dla państwa polskiego jakiejkolwiek mocy wiążącej i z jednego dokumentu normatywnego także pozbawionego mocy wiążącej dla państw członkowskich Unii Europejskiej niezwykle negatywnie świadczy o postawie polskiego projektodawcy, który zamiast chronić konstytucyjną wolność działalności gospodarczej nade wszystko polskich przedsiębiorców, ale i wolność działalności gospodarczej przypisaną mocą art. 20 Konstytucji RP także przedsiębiorcy zagranicznemu, który mógłby być uznany za dostawcę wysokiego ryzyka, wyżej stawia racje wynikające z dokumentów unijnych pozbawionych jakiejkolwiek mocy wiążącej na terenie tejże Unii Europejskiej.

Wbrew bowiem wywodom zawartym w uzasadnieniu projektu ustawy zmieniającej ustawę o KSC wprowadzenie rzeczonej instytucji stanowić będzie ograniczenie konstytucyjnej wolności działalności gospodarczej (art. 22 Konstytucji RP) albowiem w przypadku uznania dostawcy za dostawcę wysokiego ryzyka podmioty kluczowe i podmioty ważne, z wyłączeniem pochodzących z podsektora komunikacji elektronicznej, oraz przedsiębiorcy telekomunikacyjni, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe niż 10 milionów złotych:

a/ nie będą już mogły wprowadzać do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka(projektowany art. 67 c ust. 1 pkt. 1 ustawy o KSC),

b/ będą zobowiązani do wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją, a dostarczanych przez dostawcę wysokiego ryzyka w terminie 7 lat od dnia ogłoszenia lub udostępnienia informacji o przedmiotowej decyzji (projektowany art. 67 c ust. 1 pkt. 2 ustawy o KSC), także wówczas, gdy nabyły produkty ICT, procesy ICT lub usługi ICT w drodze zamówienia publicznego przed dniem ogłoszenia lub udostępnienia informacji o decyzji o uznaniu danego podmiotu za dostawcę wysokiego ryzyka (projektowany art. 67 c ust. 5 ustawy o KSC),

c/ będą zobowiązani do wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją, a dostarczanych przez dostawcę wysokiego ryzyka w terminie 5 lat od dnia ogłoszenia lub udostępnienia informacji o przedmiotowej decyzji jeżeli nabyli je w trybie zamówienia publicznego przed udostępnieniem lub ogłoszeniem informacji o decyzji o uznaniu za dostawcę wysokiego ryzyka (projektowany art. 67 c ust. 5 in fine ustawy o KSC).

Co równie ważne przedsiębiorcy telekomunikacyjni których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe niż 10 milionów złotych będą zobowiązani do wycofania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją i określonych w wykazie kategorii

funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy o KSC w ciągu 4 lat od dnia ogłoszenia lub udostępnienia informacji o przedmiotowej decyzji (projektowany art. 67 c ust. 2 ustawy o KSC).

Niewątpliwie bowiem pozbawienie podmiotów kluczowych i podmiotów ważnych oraz przedsiębiorców telekomunikacyjnych, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe niż 10 milionów złotych możliwości nabywania od konkretnych dostawców uznanych za dostawców wysokiego ryzyka typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją oraz wycofania z eksploatacji typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT objętych decyzją, a pochodzących od dostawcy wysokiego ryzyka w ciągu 7 lub 4 lat od ogłoszenia lub udostępnienia informacji o decyzji o uznaniu dostawcy za dostawcę wysokiego stanowi klasyczny wręcz przykład ograniczenia konstytucyjnej wolności działalności gospodarczej (art. 22 Konstytucji RP).

Rozważania czynione w uzasadnieniu projektu ustawy zmieniającej ustawę o KSC (str. 71 i str. 72), wedle których średni okres użytkowania sprzętu lub oprogramowania wynosi od 5- 7 lat, a w przypadku sprzętu wykorzystywanego w radiowej sieci dostępowej wynosi od 5 do 10 lat, co miałoby przemawiać za brakiem ograniczenia wolności działalności gospodarczej, skoro przedsiębiorca i tak w tym okresie czasu wymieniłby ten sprzęt lub oprogramowanie nie uwzględnia tego, iż:

a/ do ogłoszenia informacji o decyzji może dojść niewiele czasu po nabyciu sprzętu lub oprogramowania przez przedsiębiorcę, co znacząco skróciłoby możliwość jego użytkowania przez tegoż przedsiębiorcę, w stosunku do wskazanych powyżej terminów ich użytkowania,

b/ sprzęt nabyty wiele lat temu, w tym zwłaszcza wyprodukowany przez podmiot Huawei z Chińskiej Republiki Ludowej użytkowany jest przez znaczącą część przedsiębiorców telekomunikacyjnych, a także inne podmioty kluczowe lub ważne, jest sprzętem użytkowanym od bardzo wielu lat i praktycznie jest sprzętem niezawodnym działającym bezawaryjnie lub przy niezwykle niskiej awaryjności w zestawieniu z innymi tego rodzaju sprzętami i oprogramowaniem produkowanym w Unii Europejskiej lub w państwach Organizacji Paktu Północnoatlantyckiego, których to sprzęt, produkty, usługi i oprogramowanie pragnie chronić polski projektodawca.
Przymusowa zatem wymiana w pełni sprawnego, wysokiej jakości, niemalże bezawaryjnego sprzętu i oprogramowania i zastąpienie go o wiele niższej jakości, mocno awaryjnym sprzętem i oprogramowaniem pochodzącym od producentów zlokalizowanych w Unii Europejskiej lub na terenie państw Paktu Północnoatlantyckiego lub nawet w naszym kraju z jednej strony narazi przedsiębiorców na konieczność poniesienia zupełnie zbędnych, nieplanowanych do poniesienia dodatkowych kosztów, a zarazem pozostaje w pełnej sprzeczności z zasadą racjonalnego gospodarowania środkami finansowymi przez przedsiębiorców.

Należy także zważyć, że w projekcie ustawy zmieniającej ustawę o KSC nie przewidziano jakichkolwiek rekompensat dla podmiotów kluczowych, ważnych oraz przedsiębiorców telekomunikacyjnych, których przychody z działalności telekomunikacyjnej w poprzednim roku obrotowym przekroczyły 10.000.000 złotych z tytułu obowiązku wymiany produktów ICT, procesów ICT oraz usług ICT nabytych od dostawcy uznanego za dostawcę wysokiego ryzyka, co sprawi, że koszty tej wymiany w pierwszej kolejności poniosą podmioty zobowiązane do ich wymiany, a w dalszej kolejności konsumenci korzystający z ich usług (str. 30 OSR stanowiącą część składową uzasadnienia projektu ustawy zmieniającej ustawę o KSC).

Jeżeli zważymy natomiast, że przez dostawcę sprzętu lub oprogramowania projektodawca uznaje klasycznego dostawcę (importera, dystrybutora), jak i producenta oraz

upoważnionego przedstawiciela (projektowany art. 2 pkt. 4 c ustawy o KSC), to wówczas zobaczymy jak dużej liczby podmiotów dotknie decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka, który to importer, dystrybutor, ale i producent sprzętu lub oprogramowania(produktów ICT oraz procesów ICT), jak i podmiot świadczący usługi ICT zostaną pozbawieni możliwości wprowadzania na terytorium Rzeczypospolitej Polskiej produktów ICT, procesów ICT oraz usług ICT i ich sprzedawania zarówno swoim stałym odbiorcom, jak i potencjalnym nowym odbiorcom.
Taka decyzja doprowadzi do znaczącego ograniczenia rynku zbytu dla swoich usług, oprogramowania oraz sprzętu.
Niewątpliwie zatem tego rodzaju decyzja sprawi, że dojdzie do znaczącego ograniczenia konstytucyjnie gwarantowanej wolności gospodarczej także rzeczonego przedsiębiorcy zagranicznego (art. 22 Konstytucji RP).

Nie sposób także zgodzić się z poglądem projektodawcy jakoby konstytucyjna wolność działalności gospodarczej miała ustąpić przed potrzebami bezpieczeństwa państwa(str. 72 uzasadnienia projektu ustawy zmieniającej ustawę o KSC) albowiem w omawianym przypadku nie mamy do czynienia z prawem przyznanym z mocy zapisów konstytucyjnych jak np. prawo własności (art. 21 w zw. z art. 20 Konstytucji RP) lecz z wolnością działalności gospodarczej (art. 22 w zw. z art. 20 Konstytucji RP), co oznacza, że normy konstytucyjne jedynie potwierdzają ochronę wolności działalności gospodarczej, która istnieje niezależnie od zapisów konstytucyjnych, powstała niezależnie od zapisów konstytucyjnych, odmiennie niż w przypadku praw, które tworzone i przyznawane są mocą zapisów konstytucyjnych.
Konstytucja RP zatem jedynie potwierdza istnienie konstytucyjnej wolności działalności gospodarczej oraz potwierdza zapewnienie jej ochrony.
Wzmiankowane w uzasadnieniu projektu bezpieczeństwo państwa ma zatem rangę niewątpliwie niższą od wolności działalności gospodarczej, która istnieje niezależnie od istnienia państwa i niezależnie od zapisów prawnych w danym państwie obowiązujących, wynika bowiem ona niejako z prawa natury, czy też z prawa boskiego, a jej istnienie nie jest zależne od woli człowieka, odmiennie niż bezpieczeństwo państwa, które przede wszystkim wymaga stworzenia państwa wolą człowieka, a następnie stworzenie ram prawnych jego funkcjonowania, w tym i ram zakreślonych wolą człowieka dla jego bezpieczeństwa, a idąc dalej także jego cyberbezpieczeństwa.

Niewątpliwie zatem mając na uwadze powyżej zakreślony wywód natury prawnokonstytucyjnej przesądza on o tym, iż w hierarchii wartości chronionych przez Konstytucję RP wyżej stoi każda wolność, w tym i wolność działalności gospodarczej, której ochronę jedynie potwierdza Konstytucja RP w art. 22, od każdej formy bezpieczeństwa państwa.

Tym bardziej nie można zgodzić się z wywodami projektodawcy albowiem powołuje się on na niezwykle rzadko występujące, iluzoryczne wręcz postaci zagrożeń przejawiające się w atakach hakerskich oraz aktach sabotażu, czy wręcz atakach terrorystycznych organizowanych zdaniem projektodawcy przez służby wywiadowcze państw obcych oraz przez grupy przestępcze podżegane do działania na szkodę państwa polskiego przez władze lub służby wywiadowcze państw obcych(str. 72-73 uzasadnienia projektu ustawy zmieniającej ustawę o KSC)..
Iluzoryczność, a nawet wręcz marginalność zagrożeń dla bezpieczeństwa państwa polskiego, na jakie wskazuje projektodawca niewątpliwie przemawia za zapewnieniem ochrony wolności działalności gospodarczej w zestawieniu z interesem państwa polskiego wyrażającym się w ochronie jego bezpieczeństwa.

Minister właściwy do spraw informatyzacji wydaje decyzję o uznaniu dostawcy za dostawcę wysokiego ryzyka po zasięgnięciu opinii Kolegium do spraw Cyberbezpieczeństwa (projektowany art. 67 b ust. 10 ustawy o KSC).

Treść przedmiotowej opinii jest niezwykle ważna albowiem w sposób jednoznaczny ukierunkowuje nas w zamiarach polskiego projektodawcy, który wychodzi z niczym nieuzasadnionego założenia, iż dostawca wysokiego ryzyka rekrutować się będzie spośród dostawców sprzętu lub oprogramowania znajdujących się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Paktu Północnoatlantyckiego (projektowany art. 67 b ust. 11 pkt. 2 in principio ustawy o KSC).
Nie sposób zrozumieć dlaczegóż to ataki hakerskie lub akty sabotażowe, a nawet ataki terrorystyczne kierowane pod adresem podmiotów działających w naszym kraju mogą pochodzić wyłącznie od dostawców sprzętu lub oprogramowania znajdujących się pod kontrolą państw spoza terytorium Unii Europejskiej lub Organizacji Paktu Północnoatlantyckiego.
Przecież jest kwestią dowiedzioną, sojusznicy z NATO także się wzajemnie szpiegują(przykłady podsłuchów założonych przez CIA Kanclerz RFN Angeli Merkel, czy też szpiegowanie władz Wielkiej Brytanii przez służby wywiadowcze Stanów Zjednoczonych Ameryki), a zatem działania służb wywiadowczych, akty terrorystyczne i sabotażowe, czy też ataki hakerskie mogą być efektem działania władz lub służb także państw Unii Europejskiej lub Państw zrzeszonych w Organizacji NATO.

Mając z kolei na uwadze, iż dostawca sprzętu lub oprogramowania może znajdować się pod kontrolą władz państwa spoza terytorium Unii lub NATO nie można wykluczyć, że rzeczony dostawca niekoniecznie musi posiadać swoją siedzibą poza terytorium Unii lub NATO, bo przecież kontrolowanie dostawców może odnosić się także do podmiotów mających siedzibę na terytorium Unii Europejskiej lub państw zrzeszonych w NATO, w tym mających swoją siedzibę w Polsce, ale kontrolowanych przez władze państw znajdujących się poza terytorium NATO lub Unii Europejskiej.

Niezrozumiałe natomiast jest pominięcie zakresem opinii Kolegium do spraw Cyberbezpieczeństwa, a co za tym idzie i zakresem podmiotowym decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka, analizowania znajdowania się konkretnych dostawców pod kontrolą władz państwa zlokalizowanego na terytorium NATO lub Unii Europejskiej.
Przecież władze państw zrzeszonych w NATO lub wchodzących w skład Unii Europejskiej także mogą w poważnym i szerokim zakresie kontrolować dostawców sprzętu lub oprogramowania mających siedzibę na terytorium NATO lub Unii Europejskiej lub poza tym terytorium.
Dlaczego zatem projektodawca nie widzi problemu w nabywaniu przez podmioty kluczowe i ważne oraz przez pewną grupę większych przedsiębiorców telekomunikacyjnych usług ICT, produktów ICT oraz procesów ICT od dostawców znajdujących się pod kontrolą państwa z terytorium NATO lub Unii Europejskiej i tym samym wyklucza uznanie takiego dostawcy za dostawcę wysokiego ryzyka.
Przecież dla naszego kraju równie poważnym problemem może być nabywanie produktów ICT, usług ICT lub procesów ICT od dostawców znajdujących się pod kontrolą władz państw zlokalizowanych na terytorium NATO lub Unii, żeby tylko wskazać na autorytarne reżimy rządzące w państwach NATO takich jak Turcja, czy też pod kontrolą władz państw Unii Europejskiej lub NATO wielce nieprzyjaznych dla naszego państwa takich jak Niemcy, Holandia, Belgia, czy też Malta.
Te państwa mimo swojej siedziby na terytorium Unii lub NATO także mogą w wyniku kontroli dostawców sprzętu lub oprogramowania doprowadzić na terytorium naszego kraju do aktów sabotażu gospodarczego (najbardziej takimi aktami niewątpliwie mogą być zainteresowani Niemcy czujący się mocno zagrożeni wzrostem gospodarczym naszego kraju, których władze na przestrzeni dziejów zawsze były wrogo nastawione do naszego kraju i nic w tej materii zmianie nie uległo), ataków hakerskich, ataków terrorystycznych, czy też innych czynów przestępczych.
Można zapytać dlaczegóż to projektodawca nie widzi problemu w tym, że dojdzie do nabywania produktów ICT, usług ICT lub procesów ICT od dostawców znajdujących się na terytorium NATO lub Unii, nawet jeżeli podmiotom tym będą przypisane liczne akty

sabotażu, montowania podsłuchów, czy też wysyłania sprzętu elektronicznego z zamontowanymi ładunkami wybuchowymi detonowanymi w odpowiednich momentach, tylko z tego powodu, że podmioty te posiadają swoją siedzibę na terytorium państwa zrzeszonych w NATO lub w Unii Europejskiej(przykładowo wskazując w Niemczech, Królestwie Niderlandów, Belgii, czy też Hiszpanii), zaś dopuszczalne będzie uznanie za dostawcę wysokiego ryzyka dostawców z przykładowo wskazując Nigerii, Kamerunu, Bhutanu, czy też Nowej Kaledonii względnie Kostaryki, mimo iż dostawcom tym nigdy nie przypisano aktów sabotażu, zakładania podsłuchów, czy też montowania w urządzeniach elektronicznych ładunków wybuchowych następnie detonowanych zdalnie lub w odpowiednim czasie.

Takie zróżnicowane traktowanie dostawców oprogramowania i sprzętu zależnie od tego czy znajdują się pod kontrolą władz lub służb państw zlokalizowanych na terytorium Unii Europejskiej lub NATO, czy też poza tym terytorium wyrażające się w możności uznania za dostawcę wysokiego ryzyka jedynie tych dostawców produktów ICT, usług ICT lub procesów ICT, którzy znajdują się pod kontrolą władz lub służb państw zlokalizowanych poza terytorium Unii Europejskiej lub NATO, przy jednoczesnym wyłączeniu możliwości uznania za dostawcę wysokiego ryzyka dostawcy znajdującego się pod kontrolą władz lub służb państw zlokalizowanych na terytorium Unii Europejskiej lub NATO świadczy o naruszeniu wolności wykonywania działalności gospodarczej oraz równości przedsiębiorców [art. 2 ustawy z dnia 6.03.2018 r. prawo przedsiębiorców (tekst jedn .dz. U. z 2024 r. poz. 236 z późn. zm.), zwanej dalej prawem przedsiębiorców] a także o naruszeniu prawa do równego traktowania wszystkich przez władze publiczne (art. 32 ust. 1 zd. 2 Konstytucji RP) oraz konstytucyjnej zasady równości wszystkich wobec prawa (art. 32 ust. 1 zd. 1 Konstytucji RP). Co więcej, w omawianym przypadku możemy wręcz mówić o dyskryminacji jednych przedsiębiorców, a zarazem nieuprawnionym uprzywilejowaniu drugich przedsiębiorców, zależnie od terytorialnej lokalizacji państwa, którego władze lub służby danego dostawcę oprogramowania lub sprzętu kontrolują (art. 32 ust. 2 Konstytucji RP).
Takie zróżnicowanie możliwości uznania danego dostawcy za dostawcę wysokiego ryzyka zależnie od lokalizacji państwa, którego władze go kontrolują, czy znajduje się to państwo na terytorium NATO lub Unii Europejskiej, czy też poza tym terytorium nie jest możliwe także do pogodzenia z konstytucyjną zasadą sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 Konstytucji RP).

Jeżeli zatem już ma być wprowadzona instytucja dostawcy wysokiego ryzyka to powinna przybrać charakter powszechny i odnosić się wszelkich tego rodzaju dostawców także posiadających swoje siedziby na terytorium państw NATO, państw Unii Europejskiej, a nawet posiadających swoje siedziby w naszym kraju.

W tym miejscu należy także wskazać, że projektodawca w ogóle nie wziął pod uwagę możliwości naruszenia zasad uczciwej konkurencji albowiem w uzasadnieniu projektu ustawy o zmianie ustawy o KSC **brak analizy wskazującej na to, że przedmiotowa instytucja dostawcy wysokiego ryzyka eliminująca z rynku Unii Europejskiej oraz z rynku państw zrzeszonych w NATO dostawców spoza państw zlokalizowanych poza terytorium tych dwóch struktur, nie doprowadzi do zalegalizowania monopoli**, gdyż może się okazać, że na terytorium państw zrzeszonych w Pakcie Północnoatlantyckim lub w Unii Europejskiej jest to jednym dostawcy produktów ICT, usług ICT, procesów ICT, względnie niewielu więcej, którzy wówczas bez problemu mogliby pomiędzy siebie podzielić rynek, a zatem projektowana ustawa zmierza jedynie do tego by zaspokoić potrzeby naprawdę garstki dostawców produktów ICT, usług ICT, procesów ICT z obszaru NATO lub Unii Europejskiej żywotnie zainteresowanych wdrożeniem w naszym kraju instytucji dostawcy wysokiego ryzyka eliminującej z polskiego rynku ich potencjalnych konkurentów, oferujących o wiele lepszej jakości produkty ICT, procesy ICT lub usługi ICT zlokalizowanych na ich nieszczęście poza obszarem Unii Europejskiej lub NATO.

Projektodawca nie dość, że nie przeanalizował aspektów konkurencyjnych, to w dodatku swoimi propozycjami zmierza do zastąpienia na polskim rynku o wiele gorszej jakości produktami ICT, usługami ICT oraz procesami ICT pochodzący z państw Unii

Europejskiej lub NATO (np. z Malty, Cypru, Rumunii, Bułgarii, Niemiec) sprawdzonych od lat o wiele lepszej jakości produktów ICT, usług ICT oraz procesów ICT pochodzących z państw spoza NATO lub spoza Unii Europejskiej.

Koncepcja taka jest wręcz absurdalna, a zarazem niezgodna z zasadą racjonalnego gospodarowania tak gospodarką państwową, jak i przedsiębiorstwami, a nadto nie jest możliwa do pogodzenia z zasadami racjonalnego wnioskowania oraz zdrowego rozsądku.

Znajomość zasad ekonomii u polskiego projektodawcy niestety pozostawia wiele do życzenia.

Projektodawca zdecydował się na prowadzenie postepowania administracyjnego dotyczącego wydania decyzji o uznaniu danego dostawcy za dostawcę wysokiego ryzyka w oparciu o przepisy k.p.a. z wyłączeniem jednakże pewnych przepisów k.p.a.(projektowany art. 67 b ust. 2 ustawy o KSC).

Biorąc pod uwagę materię przedmiotowego postępowania możemy zaakceptować wyłączenie stosowania art. 66 a k.p.a. poświęconego metryce sprawy administracyjnej, a także regulacji art. 51 k.p.a. przewidującej obowiązek osobistego stawiennictwa się wezwanego przed organem prowadzącym postępowanie administracyjne.

Nie budzi także cienia wątpliwości uznanie za stronę postępowania administracyjnego w sprawie uznania za dostawcę wysokiego ryzyka każdego wobec kogo zostało wszczęte przedmiotowe postępowanie (projektowany art. 67 b ust. 3 ustawy o KSC).

Niestety dalsze regulacje projektu ustawy zmieniającej ustawę o KSC dotyczące uczestników postępowania administracyjnego, a także ich praw nie mogą spotkać się z naszą aprobatą.

Projektodawca jest niekonsekwentny albowiem z jednej strony wyłącza stosowanie art. 28 k.p.a. definiującego pojęcie strony postępowania administracyjnego z uwagi na to, że „*w celu usprawnienia przebiegu postepowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na względzie, że do każdego takiego postepowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania*" (str. 64 uzasadnienia projektu ustawy zmieniającej ustawę o KSC).

Argumentacja ta zasługuje na akceptację jedynie w zakresie, w którym odnosi się do ograniczenia udziału w takim akurat postępowaniu administracyjnym stron, którymi mógłby być każdy użytkownik sprzętu lub oprogramowania, a zatem tego rodzaju stron w takim postępowaniu byłyby zapewne nawet nie setki, jak pisze projektodawca, ale nawet tysiące.

Niekonsekwencja jednakże projektodawcy przejawia się w tym, iż tworzy jakąś dziwną hybrydę przyjmując, że na wniosek tegoż podmiotu na prawach strony, a więc nie w charakterze strony postępowania, do postępowania administracyjnego w sprawie o uznanie za dostawcę wysokiego ryzyka może jednakże przystąpić przedsiębiorca komunikacji elektronicznej, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego urzędu Statystycznego, o którym mowa w art. 20 pkt. 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, a którego do udziału w tymże postępowaniu dopuszcza organ postępowanie prowadzący (art. 31 § 2 k.p.a. w zw. z art. 31 § 3 k.p.a. w zw. z projektowanym art. 67 b ust. 4 ustawy o KSC).

Wykluczając bowiem z udziału w przedmiotowym postępowaniu administracyjnym prawie wszystkich użytkowników sprzętu i oprogramowania pochodzącego od osoby, wobec której wszczęto postępowanie o uznanie za dostawcę wysokiego ryzyka, które byłyby stronami tegoż postępowania w świetle regulacji art. 28 k.p.a., gdyby nie wyłączono stosowania tegoż przepisu mocą regulacji projektowanego art. 67 b ust. 2 ustawy o KSC, przy jednoczesnym dopuszczeniu do udziału w tymże postępowaniu dużego przedsiębiorcy komunikacji elektronicznej, co prawda jedynie na prawach strony (art. 31 § 2 k.p.a. w zw. z art. 31 § 3 k.p.a. w zw. z projektowanym art. 67 b ust. 4 ustawy o KSC), a nie jako stronę

postępowania administracyjnego (art. 28 k.p.a.), jest rozwiązaniem kompletnie nieakceptowalnym, a zarazem całkowicie niekonsekwentnym i kontrowersyjnym w swym wyrazie.

Przede wszystkim rozwiązanie to narusza wynikającą z konstytucji biznesu zasadę równości wszystkich przedsiębiorców (art. 2 prawa przedsiębiorców), a zarazem narusza konstytucyjną zasadę równości wszystkich wobec prawa (art. 32 ust. 1 zd. 1 Konstytucji RP) oraz konstytucyjny obowiązek równego traktowania wszystkich przez organy władzy (art. 32 ust. 1 zd. 2 Konstytucji RP).

Co więcej omawiana regulacja stanowi jaskrawy wręcz przykład dyskryminacji mniejszych przedsiębiorców wobec większych przedsiębiorców ze względu na wysokość przychodu osiąganego przez nich z realizowanej działalności gospodarczej, co jest nie do pogodzenia z normą art. 32 ust. 2 Konstytucji RP.

Trudno bowiem zrozumieć dlaczegóż to duży przedsiębiorca komunikacji elektronicznej mógłby jednak aktywnie uczestniczyć w postępowaniu administracyjnym nakierowanym na uznanie dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka korzystając z pełni praw przysługujących podmiotowi na prawach strony, gdy tymczasem mniejsi przedsiębiorcy komunikacji elektronicznej, a także pozostałe podmioty korzystające ze sprzętu lub oprogramowania pozyskanego od tegoż dostawcy mieliby być tej możliwości w majestacie prawa pozbawieni.

Wyjaśnienie bowiem dopuszczenia do udziału w tym postępowaniu na prawach strony grupy największych przedsiębiorców komunikacji elektronicznej jest niejasne, enigmatyczne, a zarazem kompletnie niezrozumiałe oraz sprzeczne z zasadami racjonalnego wnioskowania, a zapewne także po prostu nieprawdziwe, skoro projektodawca twierdzi, że w ten sposób uwzględnił postulaty strony społecznej zapewniając zarazem sprawny przebieg postępowania (str. 64-65 uzasadnienia projektu ustawy zmieniającej ustawę o KSC).

Trudno bowiem wyobrazić sobie sytuację, w której mniejsi użytkownicy sprzętu i oprogramowania postulowaliby, aby do postępowania dopuścić nieliczną grupę największych przedsiębiorców komunikacji elektronicznej z pominięciem zarazem mniejszych użytkowników sprzętu i oprogramowania pochodzącego od strony tegoż postępowania.

Jeżeli zaś za stronę społeczną uznano tę grupę nielicznych największych przedsiębiorców komunikacji elektronicznej, to mamy do czynienia z oczywistym zakłamywaniem przez projektodawcę rzeczywistości, gdyż tak niewielką grupę przedsiębiorców trudno uznać za stronę społeczną występującą o wprowadzenie tego rodzaju regulacji co zawarta w projektowanym art. 67 b ust. 4 ustawy o KSC.

W sytuacji natomiast, gdy projektodawca mógłby prowadzić postępowanie administracyjne z udziałem jednej tylko strony, do czego przyczyniło się wyłączenie stosowania art. 28 k.p.a. i art. 31 k.p.a., to trudno zgodzić się z poglądem zaprezentowanym w uzasadnieniu projektu ustawy, wedle którego zwiększenie liczby uczestników tegoż postępowania o grupę kilkunastu największych przedsiębiorców komunikacji elektronicznej zapewni sprawny przebieg postępowania.

Oczywistym wręcz jest, że prowadzenie postępowania z udziałem jednej raptem strony niewątpliwie zapewni sprawniejsze prowadzenie postępowania administracyjnego niż prowadzenie tej samej sprawy z udziałem jednakże jednej strony i dodatkowo kilkunastu podmiotów uczestniczących w postępowaniu na prawach strony.

Projektodawca zatem albo powinien dopuścić do udziału w przedmiotowym postępowaniu, i to w charakterze stron, wszystkich użytkowników sprzętu i oprogramowania pochodzących od podmiotu, wobec którego toczy się postępowanie o uznanie za dostawcę wysokiego ryzyka, niezależnie od ich wielkości i osiąganych przez nich przychodów z działalności gospodarczej albo też nie dopuścić do udziału w tymże postępowaniu ani jako stron, ani jako podmiotów na prawach strony żadnego z użytkowników sprzętu i oprogramowania pochodzących od podmiotu, którego postępowanie o uznanie za dostawcę wysokiego ryzyka dotyczy, w tym także największych przedsiębiorców komunikacji elektronicznej.

Takie rozwiązanie narusza także konstytucyjne zasady sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 w zw. z art. 8 Konstytucji RP).

Nie sposób także zaakceptować przekonania wyrażonego przez projektodawcę przemawiającego za wyłączeniem w przedmiotowym postępowaniu stosowania art. 31 k.p.a. „*w celu usprawnienia przebiegu postępowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na względzie, że do każdego takiego postepowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania*" (str. 64 uzasadnienia projektu ustawy zmieniającej ustawę o KSC), a także z powołaniem się na szczególny związek tego postępowania z kwestiami bezpieczeństwa narodowego (str. 64 uzasadnienia projektu ustawy zmieniającej ustawę o KSC).

Trudno bowiem zrozumieć w jakiż to sposób powiązanie postępowania o uznanie za dostawcę wysokiego ryzyka z kwestiami bezpieczeństwa narodowego miałoby przesądzać o potrzebie wyłączenia czynnego udziału w postępowaniu administracyjnym przez organizacje społeczne na prawach strony.

Nie przekonuje także argumentacja przemawiająca za wyeliminowaniem z udziału w postępowaniu organizacji społecznych na prawach strony, za którym to udziałem przemawia interes społeczny oraz jej cele statutowe (art. 31 § 1 in fine k.p.a.) z uwagi na potrzebę usprawnienia przebiegu postępowania oraz wzmocnienia trwałości rozstrzygnięć.

W sytuacji bowiem, gdy z postępowania przedmiotowego eliminujemy tysiące podmiotów posiadających status strony (art. 28 k.p.a.) będących użytkownikami sprzętu i oprogramowania pochodzącego od podmiotu, którego postępowanie o uznanie za dostawcę wysokiego ryzyka dotyczy, jedyną możliwość reprezentowania ich praw w tym postępowaniu zapewnia udział organizacji społecznych na prawach strony.

Pozbawienie zatem udziału w tym postępowaniu także organizacji społecznych na prawach strony jest w omawianej sytuacji kompletnie niezrozumiałe albowiem właśnie z tego powodu udział tych organizacji w postępowaniu winien być zapewniony w sposób bezdyskusyjny.

Argumentacja wskazująca na wyeliminowanie z udziału w tymże postępowaniu także organizacji społecznych na prawach strony z uwagi na potrzebę usprawnienia przebiegu postępowania upada z uwagi na jednoczesne dopuszczenie do udziału w tymże postępowaniu na prawach strony największych przedsiębiorców komunikacji elektronicznej (projektowany art. 67 b ust. 4 ustawy o KSC).

Co więcej wyeliminowanie z udziału w przedmiotowym postępowaniu organizacji społecznych na prawach strony, przy jednoczesnym zapewnieniu udziału na prawach strony kilkunastu największych przedsiębiorców komunikacji elektronicznej przesądza o naruszeniu konstytucyjnej zasady równości wszystkich wobec prawa (art. 32 ust. 1 zd. 1 Konstytucji RP), narusza konstytucyjny obowiązek równego traktowania wszystkich przez władze publiczne (art. 32 ust. 1 zd. 2 Konstytucji RP), a zarazem stanowi jaskrawy przykład dyskryminacji organizacji społecznych wobec pozycji przyznanej w projekcie największym przedsiębiorcom komunikacji elektronicznej (art. 32 ust. 2 Konstytucji RP).

Zaproponowanie przez projektodawcę tego rodzaju regulacji nie może się także ostać w świetle wymogu przestrzegania konstytucyjnej zasady sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 Konstytucji RP).

Niczego w sprawie nie zmienia zagwarantowanie wąskiej grupie organizacji społecznych (art. 5 § 2 pkt. 5 k.p.a.), a mianowicie jedynie izbom gospodarczym, prawa do przedstawienia stanowiska co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie o uznanie za dostawcę wysokiego ryzyka(projektowany art. 67 b ust. 9 ustawy o KSC) albowiem gdyby nie wyłączono stosowania w tymże postępowaniu regulacji art. 31 k.p.a.(projektowany art. 67 b ust. 2 ustawy o KSC), to izby gospodarcze, podobnie jak i pozostałe organizacje społeczne, mogłyby uczestniczyć w przedmiotowym postępowaniu administracyjnym na prawach strony korzystając z prawie wszystkich praw stronie postępowania administracyjnego przysługujących (art. 31 § 3 k.p.a.), a nie jedynie z prawa do wyrażenia opinii w sprawie zagwarantowanego organizacji społecznej w

postępowaniu administracyjnym na prawach strony nie uczestniczącej (art. 31 § 5 k.p.a.), które projektodawca przyznał jedynie izbom gospodarczym w tymże postepowaniu administracyjnym (projektowany art. 67 b ust. 9 ustawy o KSC).

Wyłączenie stosowania w postępowaniu administracyjnym o uznanie za dostawcę wysokiego ryzyka przepisu art. 79 k.p.a. zapewniającego czynny udział strony w postępowaniu dowodowym z powołaniem się na szczególny charakter tego postępowania mającego na celu zapewnienie bezpieczeństwa narodowego (str. 64 uzasadnienia projektu ustawy zmieniającej ustawę o KSC) jest nieprzekonujące, a projektodawca nie wyjaśnił w przedmiotowym uzasadnieniu w jakiż to sposób zapewnienie czynnego udziału strony w postępowaniu dowodowym prowadzonym w ramach niniejszego postępowania administracyjnego miałoby stanowić jakąkolwiek formę zagrożenia dla bezpieczeństwa narodowego.

I. W odniesieniu zatem do nowej instytucji prawnej wydania decyzji o uznaniu danego podmiotu za dostawcę wysokiego ryzyka jako główny postulat Związek Telewizji Kablowych w Polsce Izba Gospodarcza zgłasza wprowadzenie zmiany art. 1 pkt. 70 projektu ustawy zmieniającej ustawę o KSC zasadzającej się na wykreśleniu proponowanej do dodania regulacji art. 67 b- art. 67 f ustawy o KSC regulującej instytucję decyzji uznania za dostawcę wysokiego ryzyka oraz procedurę prowadzącą do wydania tej decyzji.

II. Gdyby jednakże ten najpełniejszy postulat nie został uwzględniony, to na taką okoliczność wnioskujemy o wprowadzenie zmiany art. 1 pkt. 70 ustawy zmieniającej ustawę o KSC co najmniej poprzez:

a/ wykreślenie z proponowanego art. 67 b ust. 2 ustawy o KSC zapisu wskazującego na wyłączenie stosowania w postępowaniu o uznanie za dostawcę wysokiego ryzyka art. 31 k.p.a. i art. 79 k.p.a.,

b/ wykreślenie proponowanej regulacji art. 67 b ust. 4 ustawy o KSC,

c/ wykreślenie proponowanej regulacji art. 67 b ust. 9 ustawy o KSC,

d/ wykreślenie w proponowanej regulacji art. 67 b ust. 11 pkt. 1 in fine ustawy o KSC treści w brzmieniu „*uzyskanych od państw członkowskich lub organów Unii Europejskiej lub Organizacji Paktu Północnoatlantyckiego*",

e/ wykreślenie z proponowanej regulacji art. 67 b ust. 11 ustawy o KSC pkt. 2 i pkt. 3.

Polecenie zabezpieczające

Dyrektywa NIS 2 mimo regulowania problematyki incydentów związanych z cyberbezpieczeństwem, jednakże nie przewiduje na okoliczność wystąpienia incydentu krytycznego wydawania w formie decyzji poleceń zabezpieczających, ani też nie zobowiązuje państw członkowskich do wprowadzania regulacji poświęconych instytucji poleceń zabezpieczających.

Wprowadzenie zatem do projektu ustawy zmieniającej ustawę o KSC regulacji poświęconych poleceniu zabezpieczającemu nie stanowi implementacji dyrektywy NIS 2, a zatem państwo polskie nie jest zobowiązane do wprowadzenia tego rodzaju regulacji do wewnętrznego porządku prawnego, co przesądza o tym, iż wprowadzenie tego

rodzaju regulacji nie jest obowiązkowe dla państwa polskiego w świetle normy art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej.

Propozycja zatem wprowadzenia niezwykle dolegliwej dla podmiotów ważnych i kluczowych regulacji polecenia zabezpieczającego stanowi kolejny przykład złej woli projektodawcy, który zamiast dążyć do jak najmniejszego obciążania polskich przedsiębiorców dolegliwymi regulacjami postępuje dokładnie odwrotnie dążąc ze wszystkich sił do jak najpoważniejszego ich dociążenia (projektowany art. 67 g ust. 9 ustawy o KSC).

W sytuacji zatem, gdy dyrektywa NIS 2 nie obliguje polskiego prawodawcy do wdrażania do polskiego systemu prawnego instytucji polecenia zabezpieczającego, a zatem odnośnie tej instytucji obowiązek przewidziany w art. 288 zd. 4 Traktatu o funkcjonowaniu Unii Europejskiej nie zachodzi **postulujemy wprowadzenie zmiany art. 1 pkt. 70 projektu ustawy zmieniającej ustawę o KSC poprzez wykreślenie proponowanej regulacji art. 67 g, art. 67 h, art. 67 i ustawy o KSC poświęconej problematyce polecenia zabezpieczającego**.

Uprzywilejowana pozycja Narodowego Banku Polskiego

Z sobie tylko znanych powodów projektodawca przewiduje szczególnie uprzywilejowaną pozycję Narodowego Banku Polskiego przejawiającą się w tym, że wobec przedmiotowego Banku nie znajdują zastosowania regulacje poświęcone wydaniu decyzji o uznaniu za dostawcę wysokiego ryzyka oraz skutkom płynącym z faktu wydania tego rodzaju decyzji (art. 67 b i art. 67 f ustawy o KSC), co przesądza o tym, iż nawet jeżeli konkretny podmiot zostanie uznany za dostawcę wysokiego ryzyka, to i tak Narodowy Bank Polski ani nie będzie zobowiązany do wycofania produktów ICT, usług ICT, procesów ICT w jakimkolwiek terminie, ani też nie zostanie pozbawiony możliwości na przyszłość zakupywania i stosowania od takiego dostawcy oferowanych przez niego produktów ICT, procesów ICT, czy też usług ICT.

Nie trzeba chyba nikogo przekonywać, że taka regulacja projektowanego art. 67 j ustawy o KSC narusza konstytucyjną zasadę równości wszystkich wobec prawa (art. 32 ust. 1 zd. 1 Konstytucji RP), oraz obowiązku traktowania przez władze publiczne wszystkich z poszanowaniem zasady równości (art. 32 ust. 1 zd. 2 Konstytucji RP).
Również przedmiotową regulację trudno by było uznać za zgodną z konstytucyjnymi zasadami sprawiedliwości społecznej i demokratycznego państwa prawnego (art. 2 w zw. z art. 8 Konstytucji RP).

Kierując się zasadami racjonalnego myślenia doprawdy trudno zrozumieć tego rodzaju decyzję projektodawcy, który z jednej strony przejawia olbrzymie obawy z powodu różnorakich zagrożeń dla bezpieczeństwa państwa polskiego, czemu daje wyraz także proponowaniem wprowadzenia regulacji nie będących skutkiem implementacji dyrektywy NIS 2, z drugie zaś strony nie przejawia żadnej obawy o środki finansowe i rezerwy złota zgromadzone w polskim Banku Centralnym, skoro dopuszcza do sytuacji, w której Narodowy Bank Polski przez nieograniczony okres czasu będzie korzystał z produktów ICT, usług ICT oraz procesów ICT pochodzących od dostawcy wysokiego ryzyka.

Co więcej, w sytuacji przykładowo wskazując zhakowania procesów, w tym oprogramowania, stosowanych przez Bank Centralny właśnie z tego powodu, że zastosowano procesy ICT, potencjalny haker uzyska dostęp za pośrednictwem NBP do zasobów innych banków powiązanych z Bankiem Centralnym systemami teleinformatycznymi chociażby związanymi z procedurą udzielania im przez NBP kredytu refinansowego, a poprzez kolejne banki komercyjne tą samą drogą rzeczony haker uzyska dostęp do danych osobowych oraz środków wszystkich klientów tychże banków zgromadzonych przez te banki, a to tylko z tego powodu, że z sobie znanych motywów, niestety nie wyjaśnionych w uzasadnieniu projektu ustawy o zmianie ustawy o KSC,

projektodawca postanowił wyłączyć Narodowy Bank Polski z zastosowania wobec niego instytucji dostawcy wysokiego ryzyka.

Kierując się zasadami racjonalnego myślenia, względami słuszności oraz naruszeniem przytoczonych powyżej norm konstytucyjnych zdecydowanie **optujemy za usunięciem z ustawy o KSC uprzywilejowanej pozycji Narodowego Banku Polskiego i z tego właśnie powodu wnosimy o wprowadzenie zmiany art. 1 pkt. 70 projektu ustawy zmieniającej ustawę o KSC poprzez wykreślenie projektowanego przepisu art. 67 j ustawy o KSC.**

Ocena niniejsza wraz ze stosownymi uwagami i wnioskami w takiej samej formie została przez naszą Izbę Gospodarczą skierowana do: Sekretarza Stanu w Ministerstwie Cyfryzacji Pana Pawła Olszewskiego, Dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji Pana Łukasza Wojewody, Ministra Rozwoju i Technologii Pana Krzysztofa Paszyka, Rzecznika Małych i Średnich Przedsiębiorców Pani Agnieszki Majewskiej oraz nade wszystko do Prezesa Rady Ministrów Pana Donalda Tuska.

Licząc na to, że projektodawca uwzględni nasze postulaty zapewniamy zarazem, że proponowanej regulacji na etapie prac parlamentarnych nasza Izba Gospodarcza z pewnością nie poprze podejmując usilne starania zmierzające w pierwszej kolejności do wyeliminowania z projektu ustawy o zmianie ustawy o KSC wielce szkodliwych dla gospodarki rodzimej i polskich przedsiębiorców instytucji: dostawcy wysokiego ryzyka oraz polecenia zabezpieczającego.

Z wyrazami szacunku

Prezes Zarządu

Paweł Wołoch

Signature Not Verified

Dokument podpisany
przez Paweł Wołoch
Data: 2025.01.18
18:53:44 CET