Do druku nr 1955

KRAJOWA IZBA KOMUNIKACJI ETHERNETOWEJ

ul. Lindleya 16, 02-013 Warszawa
tel. + 48 22 2928700, fax +48 22 2928701
www.kike.pl, e-mail: biuro@kike.pl, grap@kike.pl
KRS 0000316678, REGON 141637224, NIP 9512270210

Warszawa, dnia 2 grudnia 2025 r.

DKKIKE-2130

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. nadregulacji w *projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk nr 1955)*

Szanowny Panie Marszałku,

w imieniu członków Krajowej Izby Komunikacji Ethernetowej (KIKE, Izba), zrzeszającej polskich małych i średnich przedsiębiorców telekomunikacyjnych[1] (MŚP) i zarazem największej izby (pod względem liczby członków) branży telekomunikacyjnej, zwracam się do Pana Marszałka z prośbą o rozpatrzenie oraz o przekazanie Posłom Sejmu RP **apelu KIKE o usunięcie nadregulacji *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*** (Projekt ustawy).

Celem Projektu ustawy jest wdrożenie prawa UE, przede wszystkim dyrektywy NIS2. Wdrożenie praw UE jest potrzebne. Niestety, Projekt ustawy zawiera również rozwiązania wykraczające poza wymogi prawa UE (nadregulacja).

KIKE protestuje przeciwko nakładaniu na Polaków obowiązków, które:

1) nie spoczywają na przedsiębiorcach z innych państw członkowskich UE,

2) dyskryminują przedsiębiorców MŚP i m.in. w tym zakresie są niezgodne z Konstytucją RP (naruszenie zasady proporcjonalności, naruszenie istoty prawa własności, zasady rzetelności i sprawności instytucji publicznych) – w załączeniu wysyłamy opinię prof. dr hab. Ryszarda Piotrowskiego (przygotowaną na zlecenie KIKE), jednego z najbardziej znanych autorytetów z zakresu prawa konstytucyjnego w naszym kraju.

Do niniejszego pisma załączamy propozycje konkretnych poprawek, które zmierzają do tego, aby usunąć z Projektu ustawy szkodliwą dla polskich przedsiębiorców nadregulację.

Z poważaniem

Karol Skupień

Prezes Zarządu KIKE

Załączniki:
1) tabela z propozycjami poprawek KIKE zmierzającymi do usunięcia nadregulacji z Projektu ustawy, wraz z uzasadnieniem,
2) opinia prof. dr hab. Ryszarda Piotrowskiego o zgodności wybranych przepisów Projektu ustawy z Konstytucją RP.

[1] https://kike.pl/czlonkowie/

Razem możemy więcej!

Załącznik nr 1 do apelu Krajowej Izby Komunikacji Ethernetowej z 2.12.2025 r. o usunięcie nadregulacji z projektu nowelizacji KSC (druk nr 1955)

Tabela z propozycjami poprawek KIKE zmierzającymi do usunięcia nadregulacji z Projektu ustawy

Lp.	Propozycja poprawki	Uzasadnienie
	Zagadnienie: zawyżone sankcje i zbyt długi czas polecenia zabezpieczającego	
1.	W art. 1 w pkt 16 w art. 8 ust. 3 nadać brzmienie: „3. Podmiot ważny nie stosuje przepisu ust. 1. Podmiot ważny opracowuje, wdraża, realizuje, monitoruje i utrzymuje w systemach informacyjnych kontrolowanych przez ten podmiot system zarządzania bezpieczeństwem informacji spełniający wymogi określone w załączniku nr 4 do ustawy". ***Uwaga: poprawkę nr 1 należy głosować łącznie z poprawkami nr 10-15***	Dyrektywa NIS2 w swoim art. 2 ust. 2 lit. b-f pozostawia pewien zakres swobody państwom członkowskim w zakresie katalogu podmiotów, w szczególności publicznych, które powinny spełniać wymogi określone w dyrektywnie, w tym m.in. w jej art. 21. W sytuacji, gdy dany podmiot zostanie już jednak zakwalifikowany jako kluczowy lub ważny, dyrektywa, w art. 21, nie różnicuje obowiązków spoczywających na podmiotach kluczowych lub ważnych, w zależności od tego, czy są to podmioty prywatne, czy publiczne. Inaczej sytuacja przedstawia się w przypadku środków nadzoru i egzekwowania przepisów. Przykładowo, art. 32 ust. 5 akapit trzeci dyrektywy NIS2, wskazuje wprost, że *„środki egzekwowania przepisów określone w niniejszym ustępie nie mają zastosowania do podmiotów administracji publicznej objętych zakresem niniejszej dyrektywy"*. Zatem tam, gdzie takie różnicowanie jest dopuszczalne, dyrektywa wskazuje to wprost. Także art. 34 ust. 7 dyrektywy NIS2 w dopuszcza odmienne traktowania podmiotów publicznych w porównaniu z podmiotami prywatnymi. W przypadku spełniania wymogów z art. 21 dyrektywy NIS2 nie przewidziano jednak uprzywilejowania dla podmiotów publicznych. W związku z powyższym, jeżeli w przypadku podmiotów ważnych, będących podmiotami publicznymi, wystarczające jest spełnienie wymogów określonych w załączniku nr 4 zamiast spełnienia wymogów wskazanych w art. 8 KSC, powinno być ono wystarczające także w przypadku podmiotów ważnych, będących podmiotami prywatnymi.

		Konsekwencją uwzględnienia uwagi jest konieczność dokonania poprawek legislacyjnych w załączniku nr 4 do Projektu ustawy. *** ***Poprawka 1 naniesiona na aktualne brzmienie Projektu ustawy***: Art. 1 . W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069) wprowadza się następujące zmiany: [...] 16) art. 8 otrzymuje brzmienie: [...] „3. Podmiot ważny ~~będący podmiotem publicznym~~ nie stosuje przepisu ust. 1. Podmiot ważny ~~będący podmiotem publicznym~~ opracowuje, wdraża, realizuje, monitoruje i utrzymuje w systemach informacyjnych kontrolowanych przez ten podmiot system zarządzania bezpieczeństwem informacji spełniający wymogi określone w załączniku nr 4 do ustawy."
2.	W art. 1 w pkt 76 w art. 76g ust. 12 otrzymuje brzmienie: „12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego." ***Uwaga: poprawkę nr 2 należy głosować łącznie z poprawką nr 3***	O ile KIKE dostrzega potrzebę szybkiej i skutecznej reakcji w przypadku zaistnienia incydentu krytycznego, o tyle niektóre z nakazów, które mogą zostać zawarte w takim poleceniu są bardzo dotkliwe i powinny obowiązywać tak krótko, jak to tylko możliwe. Przykładowo, skoro jednym z nakazów może być „nakaz wprowadzenia ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego" (projektowany art. 67g ust. 10 pkt 7 KSC), gdyby takie ograniczenie ruchu sieciowego miało trwać dwa lata (a nawet i 6 miesięcy, gdyby był to podmiot, dla którego ruch sieciowy jest niezbędny dla prowadzenia działalności), wówczas podmiot, którego ruch przychodzący miałby zostać ograniczony, z pewnością byłby zmuszony do zakończenia działalności gospodarczej. Zgodnie z art. 32 ust. 4 lit. b dyrektywy NIS2, właściwe organy państwa członkowskiego powinny być uprawnione m.in. do wydawania wiążących poleceń, w tym dotyczących podjęcia środków niezbędnych do usunięcia skutków incydentu. Tymczasem, w opinii KIKE, jedynym słusznym rozwiązaniem, które faktycznie mogłoby służyć zapewnieniu cyberbezpieczeństwa, byłoby zastosowanie polecenia zabezpieczającego wyłącznie do czasu zakończenia koordynacji obsługi incydentu.
3.	W art. 1 w pkt 76 w art. 76g ust. 13 otrzymuje brzmienie: „13. Polecenie zabezpieczające wygasa z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, jednak nie później niż po dwóch latach od jego wydania." ***Uwaga: poprawkę nr 3 należy głosować łącznie z poprawką nr 2***	

		Aktualne rozwiązanie dopuszcza sytuację, gdy polecenie zabezpieczające może być w mocy nawet wówczas, gdy zagrożenie (incydent krytyczny) minęło, co stanowiłoby zaprzeczenie zasady proporcjonalności (o której mowa w art. 67 ust. 4 Prawa przedsiębiorców) oraz wykracza poza środki „niezbędne", o których mowa w art. 32 ust. 4 dyrektywy NIS2. *** ***Poprawki 2 i 3 naniesione na aktualne brzmienie Projektu ustawy***: „76) po rozdziale 12 dodaje się rozdział 12a w brzmieniu: [...] Art. 67g. [...] 12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego ~~lub na czas oznaczony, nie dłużej niż na dwa lata~~. 13. Polecenie zabezpieczające wygasa~~:~~ ~~1)~~ z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, **jednak nie później niż po dwóch latach od jego wydania** ~~lub~~ ~~2) po upływie czasu, na który zostało wydane~~."
4.	W art. 1 w pkt 82 w lit. d w art. 73 w ust. 3 otrzymuje brzmienie: „3. . Wysokość kary pieniężnej nie może przekroczyć 10 000 000 euro, wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku	**Uzasadnienie poprawek 4-6:** Zgodnie z art. 34 ust. 4 i 5 dyrektywy NIS2[2], wdrażanej Projektem ustawy" *„4. Państwa członkowskie zapewniają, by podmioty kluczowe dokonujące naruszeń art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 10 000 000 EUR lub co najmniej 2 %*

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)

	obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa."	*łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot kluczowy, przy czym zastosowanie ma kwota wyższa.* *5. Państwa członkowskie zapewniają, by podmioty ważne dokonujące naruszeń art. 21 lub 23 podlegały zgodnie z ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 7 000 000 EUR lub 1,4 % łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot ważny, przy czym zastosowanie ma kwota wyższa.".*
5.	W art. 1 w pkt 82 w lit. d w art. 73 w ust. 4 otrzymuje brzmienie: „4. Wysokość kary pieniężnej nie może przekroczyć 7 000 000 euro, wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 1,4% przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Przepis ust. 3a stosuje się odpowiednio z zastrzeżeniem, że za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 250 000 euro."	Maksymalne progi kar pieniężnych, przewidziane w art. 34 ust. 4 i 5 dyrektywy NIS2 są już bardzo wysokie, jak na warunki prowadzenia działalności gospodarczej w Polsce. Przepisy te nie przewidują: - ani minimalnej wysokości kary, - ani podwyższonego progu maksymalnego kary w jakichkolwiek szczególnych sytuacjach. Próg w wysokości 100 000 000 zł wyraźnie przekracza maksymalne, i tak już wysokie progi kar pieniężnych, które dyrektywa NIS2 przewiduje dla podmiotów kluczowych i ważnych. Co więcej, ani kara minimalna (15 000 zł w przypadku podmiotów ważnych, czy 20 000 zł w przypadku podmiotów kluczowych), ani kara „do 100 000 000 zł" nie jest w żaden sposób powiązana z wysokością obrotu karanego przedsiębiorcy. Należy podkreślić, że zarówno do podmiotów kluczowych, jak i podmiotów ważnych mogą zostać zaliczeni – w przypadku niektórych sektorów – nawet mikroprzedsiębiorcy. Przykładowo, przedsiębiorcy komunikacji elektronicznej będący mikro- lub małymi przedsiębiorcami, zostaną zakwalifikowani jako podmioty ważne (projektowany art. 5 ust. 2 pkt 3 KSC). Mikro, mali i średni przedsiębiorcy komunikacji elektronicznej stanowią zdecydowaną większość w podsektorze komunikacji elektronicznej (przy czym średni przedsiębiorcy komunikacji elektronicznej będą kwalifikowani już jako podmioty kluczowe: por. projektowany art. 5 ust. 1 pkt 2 KSC). Zgodnie z Raportem Prezesa Urzędu

6.	W art. 1 w pkt 82 w lit. d w art. 73 skreśla się ust. 5.	Komunikacji Elektronicznej o stanie rynku telekomunikacyjnego w 2024 r. Rynek telekomunikacyjny pod względem ilości podmiotów zdominowany jest przez małe i średnie przedsiębiorstwa. MŚP stanowią 99,4% ogólnej liczby przedsiębiorców telekomunikacyjnych działających na polskim rynku. Dla mikroprzedsiębiorców kara minimalna za pojedyncze naruszenie w wysokości 15 000 zł, oderwana od rzeczywistej wielkości przychodów i dochodów przedsiębiorcy, może doprowadzić nawet do jego upadłości. Tymczasem podmiot naruszający przepisy ustawy w pierwszej kolejności powinien móc przeznaczyć środki finansowe na naprawienie swoich błędów, a nie na zapłacenie kary. *** ***Poprawki 2-4 naniesione na aktualne brzmienie Projektu ustawy***: 82) w art. 73: [...] d) ust. 3 otrzymuje brzmienie: „3. Wysokość kary pieniężnej nie może przekroczyć 10 000 000 euro, wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa. ~~Kara ta nie może być jednak niższa niż 20 000 zł.~~", [...] f) ust. 4 i 5 otrzymują brzmienie: „4. Wysokość kary pieniężnej nie może przekroczyć 7 000 000 euro, wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 1,4% przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. ~~Kara ta nie może być jednak niższa niż 15 000 zł~~. Przepis ust. 3a stosuje się odpowiednio z zastrzeżeniem, że za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 250 000 euro. ~~5. Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując:~~

		~~1) bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,~~ ~~2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług~~ ~~– organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 100 000 000 zł~~.”

7.	W art. 1 w pkt 84 w art. 74 ust. 4 otrzymuje brzmienie: „4. Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności". ALBO W art. 1 w pkt 84 w art. 74 skreśla się ust. 4.	KIKE postuluje nadanie projektowanemu art. 74 ust. 4 KSC wskazanego brzmienia, albo ewentualnie wykreślenie tego ustępu w całości. Należy podkreślić, że zgodnie z art. 108 § 1 Kodeksu postępowania administracyjnego (KPA) *„Decyzji, od której służy odwołanie, może być nadany rygor natychmiastowej wykonalności, gdy jest to **niezbędne ze względu na ochronę zdrowia lub życia ludzkiego albo dla zabezpieczenia gospodarstwa narodowego przed ciężkimi stratami bądź też ze względu na inny interes społeczny lub wyjątkowo ważny interes strony**.".* Ogólne zasady nałożenia rygoru natychmiastowej wykonalności na decyzje administracyjne, zgodnie z KPA, są dużo bardziej surowe niż przewidziane w Projekcie ustawy. Innymi słowy, **wielokrotnie łatwiej będzie nałożyć rygor natychmiastowej wykonalności na decyzję nakładającą karę pieniężną na podstawie KSC niż – co do zasady – w jakiejkolwiek innej sprawie.** Należy wziąć pod uwagę, że koszty wdrożenia wymogów dyrektywy NIS2. Firma EY szacuje te koszty w granicach od kilkudziesięciu tysięcy złotych dla mniejszych firm do milionów złotych dla większych podmiotów[3]. Z kolei zdaniem firmy Netia, **miesięczny koszt wydatków na sam Security Operations Centre** (struktury odpowiedzialne za cyberbezpieczeństwo) wynosi **kilkadziesiąt tysięcy złotych miesięcznie[4].** Zgodnie z art. 446 ust. 1 zdanie drugie Prawa komunikacji elektronicznej (PKE) „Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności". Podobne rozwiązanie powinno zostać ujęte w KSC. Realizacja obowiązków wynikających z dyrektywy NIS2/KSC będzie z pewnością kosztowna dla każdego przedsiębiorcy. W przypadku, gdy przedsiębiorca niektórych z tych obowiązków nie zrealizuje albo zrobi to w sposób niepełny, w pierwszej kolejności powinien mieć możliwość przeznaczenia swoich środków pieniężnych na realizację tych obowiązków zamiast na zapłatę kary pieniężnej. W przeciwnym razie **kara pieniężna zamiast mobilizować przedsiębiorcę może uniemożliwić mu realizację obowiązków**. ***

[3] Raport Telko.in "Wdrożenie przepisów ustawy o krajowym systemie cyberbezpieczeństwa. Technologiczne i prawne wyzwania", str. 7-8; https://www.telko.in/download,11719

[4] https://www.netia.pl/pl/srednie-i-duze-firmy/produkty/bezpieczenstwo/netia-soc

		Poprawka 7 naniesiona na aktualne brzmienie Projektu ustawy: 84) art. 74 otrzymuje brzmienie: [...] „4. **Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.** ~~Organ właściwy do spraw cyberbezpieczeństwa lub właściwy organ w rozumieniu rozporządzenia 2022/2554 może decyzji, o której mowa w ust. 1 lub ust. 3, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego~~."
8.	W art. 1 w pkt 86 skreśla się art. 76b. ***Uwaga: poprawkę nr 8 należy głosować łącznie z poprawką nr 9***	Dyrektywa NIS2 w art. 35 ust. 6 dopuszcza stosowanie kar okresowych: *„6. Państwa członkowskie **mogą** przewidzieć uprawnienie do nakładania okresowych kar pieniężnych w celu przymuszenia podmiotu kluczowego lub ważnego do zaprzestania naruszenia niniejszej dyrektywy zgodnie z wcześniejszą decyzją właściwego organu".* Dyrektywa NIS2 dopuszcza zatem okresowe kary pieniężne, lecz ich nie wymaga. Skorzystanie z tej możliwości stanowi zatem nadregulację. Wysokie kary za naruszenia przepisów KSC, w połączeniu z szerokim katalogiem środków nadzorczych powodują, że okresowe kary pieniężne nie są niezbędne w celu skutecznego przymuszenia podmiotów kluczowych i ważnych do przestrzegania obowiązków wynikających z KSC. *** ***Poprawka 8 naniesiona na aktualne brzmienie Projektu ustawy***: 86) po art. 76 dodaje się art. 76a–76e w brzmieniu: [...] „[...] ~~Art. 76b. 1. Niezależnie od kary pieniężnej nałożonej na podstawie art. 73 ust. 1, organ właściwy do spraw cyberbezpieczeństwa, w celu przymuszenia podmiotu kluczowego albo~~
9.	W art. 1 w pkt 86 art. 76c, art. 76d i art. 76e otrzymują numerację art. 76b, art. 76c i art. 76d. ***Uwaga: poprawkę nr 9 należy głosować łącznie z poprawką nr 8***	

		~~podmiotu ważnego do wykonania nałożonych na niego obowiązków, może nałożyć na ten podmiot, w drodze decyzji, okresową karę pieniężną w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia, w wykonaniu decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–8.~~ ~~2. Okresową karę pieniężną nakłada się, licząc od daty wskazanej w decyzji o nałożeniu tej kary.~~ ~~3. Do okresowej kary pieniężnej stosuje się przepisy art. 74 ust. 4 i 5~~."
10.	Tytuł załącznika nr 4 otrzymuje brzmienie: „WYMOGI DLA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI DLA PODMIOTU WAŻNEGO"	Zmiany legislacyjne, wynikające z uwzględnienia poprawki nr 1. Uzasadnienie tożsame z uzasadnieniem poprawki nr 1.
11.	W załączniku nr 4 w pkt. I wprowadzenie do wyliczenia otrzymuje brzmienie: „System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej:"	
12.	W załączniku nr 4 w pkt. II wprowadzenie do wyliczenia otrzymuje brzmienie: „System zarządzania bezpieczeństwem informacji dla podmiotu ważnego może dodatkowo obejmować:"	
13.	W załączniku nr 4 w pkt. II wprowadzenie do wyliczenia otrzymuje brzmienie: „4) określanie i kontrolowanie zasad korzystania przez podmiot ważny z:"	
14.	W załączniku nr 4 w pkt. III wprowadzenie do wyliczenia otrzymuje brzmienie:	

	„Podmiot ważny dokonuje przeglądu systemu zarządzania bezpieczeństwem informacji:"	
15.	W załączniku nr 4 pkt IV otrzymuje brzmienie: „Podmiot ważny dokumentuje realizacje działań wskazanych do realizacji w systemie zarządzania cyberbezpieczeństwa."	
	Zagadnienie: Zbyt szeroki obowiązek usuwania sprzętu od dostawcy wysokiego ryzyka (DWR)	
	Część wspólna uzasadnienia poprawek nr 16-26: Koncepcja DWR wynika z publikacji „5G Toolbox"[5], a nie z aktu prawnego. 5G Toolbox to raport o dostępnych narzędziach (tools) minimalizowania ryzyka w sieciach 5G. Przepisy o DWR nie są transpozycją dyrektywy NIS22, lecz zaleceń 5G Toolbox. **DWR to nie jest narzędzie do zwalczania podmiotów odpowiedzialnych lub współodpowiedzialnych za cyberataki**. Takiemu celowi służy rozporządzenie 2019/796 i Kodeks karny. Wspomniane rozporządzenie przewiduje dotkliwe sankcje, w tym blokadę środków finansowych dla podmiotów odpowiedzialnych za cyberataki oraz podmiotów, które je wspierały. Z kolei usuwanie groźnych wad sprzętu (podatności) powinno być dokonywane na podstawie art. 32 ust. 2 KSC – takie rozwiązanie jest przewidziane nawet już w obowiązującej ustawie. **DWR w 5G Toolbox służy wyłącznie zarządzaniu ryzykiem w kontroli dostępu oraz zakłóceń w łańcuchu dostaw dla sieci 5G.** W dokumencie 5G Toolbox, na którym oparto rozwiązania dotyczące decyzji DWR, podkreśla się wyjątkową rolę sieci wykonanej w technologii 5G oraz szczególny charakter więzi pomiędzy dostawcami sprzętu i oprogramowania a operatorami świadczącymi usługi komunikacji elektronicznej w sieci 5G. Takiego powiązania nie ma w przypadku sieci wykonanej w innych technologiach (w szczególności w przypadku sieci stacjonarnych), ani w przypadku pozostałych 17 sektorów gospodarki, których dotyczy Projekt ustawy, a w 5G Toolbox nie ma o nim mowy. **W związku z powyższym, rozciągnięcie obowiązku usuwania sprzętu i oprogramowania dostawcy DWR na sieci inne niż wykonane w technologii 5G oraz na podmioty inne niż operatorzy 5G stanowi nadregulację.**	

[5] "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures"; autor: Grupa Współpracy NIS, działająca na podstawie decyzji Komisji Europejskiej 2017/179.

16.	W art. 1 w pkt 76 w art. 67b ust. 1 otrzymuje brzmienie: „1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć, z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania, które są wykorzystywane przez przedsiębiorców komunikacji elektronicznej dostarczających sieć piątej generacji (5G), określoną w dokumencie technicznym - Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) lub dokumencie go zastępującym oraz pełniące w sieci 5G funkcje określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci 5G w załączniku nr 3 do ustawy, za dostawcę wysokiego ryzyka."	Poprawka zmierza do prawidłowego określenia katalogu podmiotów, których powinien dotyczyć obowiązek wycofywania sprzętu i oprogramowania DWR w użytkowania. Takimi podmiotami są tylko operatorzy sieci telekomunikacyjnej 5G, ze względu na jej właściwości techniczne i wrażliwość na relacje z dostawcami. Co więcej, zgodnie z 5G Toolbox, obowiązek usuwania sprzętu i oprogramowania (i to w niezbędnym zakresie! – o czym będzie mowa później) powinien dotyczyć wyłącznie tego sprzętu i oprogramowania, które w sieci 5G pełni funkcje krytyczne. *** ***Poprawka 16 naniesiona na aktualne brzmienie Projektu ustawy***: „Art. 67b. 1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć, z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania, które są wykorzystywane przez: ~~1) podmioty kluczowe lub podmioty ważne, z wyłączeniem podsektora komunikacji elektronicznej,~~ ~~2)~~ przedsiębiorców komunikacji elektronicznej **dostarczających sieć piątej generacji (5G), określoną w dokumencie technicznym - Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) lub dokumencie go zastępującym oraz pełniące w sieci 5G funkcje określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci 5G w załączniku nr 3 do ustawy**~~których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych,~~ ~~3) podmioty finansowe, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554~~ – za dostawcę wysokiego ryzyka."
17.	W art. 1 w pkt 76 w art. 67b ust. 2 otrzymuje brzmienie: „2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, jeżeli ustawa nie stanowi inaczej, stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego."	Najważniejszym skutkiem decyzji DWR jest nakaz usuwania całych kategorii sprzętu i oprogramowania DWR bez odszkodowania (projektowany art. 67c ust. 1 KSC). Ten obowiązek miałby spoczywać na wszystkich podmiotach, które podlegają pod przepisy KSC, przy czym nie na przedsiębiorcach komunikacji elektronicznej o rocznych

		przychodach poniżej 10 mln zł – a zatem nie na mikroprzedsiębiorcach oraz nie na najmniejszych spośród przedsiębiorców małych. Tymczasem w podstępowaniu w sprawie uznania dostawcy za DWR może brać udział sam dostawca (projektowany art. 67b ust. 3 KSC) oraz może przystąpić, na prawach strony (czyli z możliwością zapoznawania się z argumentami strony przeciwnej i przedstawiania swojego stanowiska w odniesieniu do tych pojawiających się w postępowaniu różnorodnych argumentów) **TYLKO PRZEDSIĘBIORCA TELEKOMUNIKACYJNY KTÓRY W POPRZEDNIM ROKU OBROTOWYM UZYSKAŁ PRZYCHÓD** Z TYTUŁU PROWADZENIA DZIAŁALNOŚCI TELEKOMUNIKACYJNEJ W WYSOKOŚCI CO NAJMNIEJ DWUDZIESTOTYSIĘCZNEJ KROTNOŚCI PRZECIĘTNEGO WYNAGRODZENIA W GOSPODARCE NARODOWEJ, CZYLI **PONAD 160 000 000 zł** (projektowany art. 67b ust. 4 KSC). Projektowane rozwiązanie DWR wprowadza zatem cenzus majątkowy – tylko przedsiębiorcy, i to **wyłącznie przedsiębiorcy telekomunikacyjni** (w przeciwieństwie do przedsiębiorców ze wszystkich innych branż podlegających pod KSC), **spełniający bardzo wysoki cenzus majątkowy będą mieć prawo przystąpienia do postępowania DWR na prawach strony**. Brak prawa dla mniejszych podmiotów, na których będzie spoczywał taki sam obowiązek, wyłącznie ze względu na to, że są „zbyt biedni" w porównaniu z kilku lub kilkunastoma największymi podmiotami na rynku woła o pomstę do Nieba. Projektowany art. 67b ust. 2 zakłada obecnie, że następujące przepisy KPA nie będą mogły znaleźć zastosowania w postępowaniu mającym ustalić, czy dany dostawca powinien zostać uznany za DWR: 1) art. 28 Kodeksu postępowania administracyjnego (KPA) „Stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie albo kto żąda czynności organu ze względu na swój interes prawny lub obowiązek." – czyli stroną nie może zostać żaden podmiot, którego interesu prawnego dotyczy wynik postępowania DWR (nakaz wycofania sprzętu z użytkowania i zakaz kupowania nowego sprzętu) nie może brać aktywnego udziału w postępowaniu, czyli przede wszystkim odnosić się do argumentów strony przeciwnej – z wyjątkiem kilku uprzywilejowanych, bo największych przedsiębiorców telekomunikacyjnych;

		2) art. 31 KPA – czyli argumenty MŚP (oraz podmiotów spoza sektora komunikacji elektronicznej) przedstawiane w odpowiedzi na stanowiska strony przeciwnej nie będą mogły być prezentowane nawet za pośrednictwem organizacji społecznej; 3) art. 51 KPA – obowiązek osobistego stawiennictwa i jego ograniczenie; 4) art. 66a KPA – metryka sprawy – zgodnie z art. 66a § 2 KPA „ W treści metryki sprawy wskazuje się wszystkie osoby, które uczestniczyły w podejmowaniu czynności w postępowaniu administracyjnym oraz określa się wszystkie podejmowane przez te osoby czynności wraz z odpowiednim odesłaniem do dokumentów określających te czynności". W postępowaniu o skutku w postaci **wywłaszczenia bez odszkodowania** jest szczególnie ważne, aby wszelkie czynności, które mogą mieć wpływ na wynik postępowania, były dokumentowane; 5) art. 79 KPA stanowi, że „ § 1. Strona powinna być zawiadomiona o miejscu i terminie przeprowadzenia dowodu ze świadków, biegłych lub oględzin przynajmniej na siedem dni przed terminem./ § 2. Strona ma prawo brać udział w przeprowadzeniu dowodu, może zadawać pytania świadkom, biegłym i stronom oraz składać wyjaśnienia."; są to podstawowe prawa stron w postępowaniu, niezbędne do ustalenia prawny obiektywnej. Wyłączenie tak podstawowych gwarancji procesowych w postępowaniu stawia pod znakiem zapytania rzetelność całego postępowania. *** ***Poprawka 17 naniesiona na aktualne brzmienie Projektu ustawy***: „Art. 67b [...] 2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, jeżeli ustawa nie stanowi inaczej, stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego~~, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy~~."
18.	W art. 1 w pkt 76 w art. 67b skreśla się ust. 4.	To projektowany art. 67b ust. 4 KSC stanowi, że do podstępowania w sprawie uznania dostawcy za DWR może przystąpić, na prawach strony **TYLKO PRZEDSIĘBIORCA TELEKOMUNIKACYJNY KTÓRY W POPRZEDNIM ROKU OBROTOWYM UZYSKAŁ PRZYCHÓD** Z TYTUŁU PROWADZENIA DZIAŁALNOŚCI TELEKOMUNIKACYJNEJ W WYSOKOŚCI CO NAJMNIEJ DWUDZIESTOTYSIĘCZNEJ KROTNOŚCI PRZECIĘTNEGO

	Uwaga: poprawkę nr 18 należy głosować łącznie z poprawką nr 19	WYNAGRODZENIA W GOSPODARCE NARODOWEJ, CZYLI **PONAD 160 000 000 zł** (projektowany art. 67b ust. 4 KSC). Tak rażący przejaw dyskryminacji MŚP powinien być z projektu ustawy w całości usunięty. *** ***Poprawka 18 naniesiona na aktualne brzmienie Projektu ustawy***: Art. 67b [...] ~~4. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka może przystąpić, na wniosek, na prawach strony, przedsiębiorca telekomunikacyjny mający siedzibę na terytorium Rzeczypospolitej Polskiej wpisany do rejestru przedsiębiorców telekomunikacyjnych, 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 (Dz. U. z 2024 r. poz. 1631 i 1674 oraz z 2025 r. poz. 718, 769 i 1159). Przepisy art. 31 § 2 i 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio~~.".
19.	W art. 1 w pkt 76 w art. 67b skreśla się ust. 5. ***Uwaga: poprawkę nr 19 należy głosować łącznie z poprawką nr 18***	W razie skreślenia projektowanego art. 67b ust. 4, przepis ust. 5 staje się bezprzedmiotowy. *** ***Poprawka 19 naniesiona na aktualne brzmienie Projektu ustawy***: „Art. 67b [...] 5. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego ogłoszony przed wszczęciem postępowania."
20.	W art. 1 w pkt 76 w art. 67b w ust. 10 skreśla się zdanie ostatnie.	Zgodnie z projektowanym art. 67b ust. 10 KSC przed wydaniem decyzji minister właściwy do spraw informatyzacji zasięga opinii Kolegium ds. cyberbezpieczeństwa. Kolegium

		przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Standardową zasadą w takim przypadku wyrażoną w KPA, jest możliwość wniesienia zażalenia na taką opinię, czy też wyrażenia stanowiska przez inny organ w innej formie. Możliwość wniesienia zażalenia powinna istnieć, ponieważ opinia Kolegium powinna zawierać analizę bardzo wielu kwestii, a wiele z nich dotyczy praktycznych aspektów funkcjonowania dostawcy na rynku. Kontrahenci danego dostawcy z pewnością mogą dysponować szeroką wiedzą na temat dostawcy, z którego sprzętu i oprogramowania korzystają. Powinni mieć zatem prawo wniesienia zażalenia na opinię Kolegium, gdyby miało okazać się, że zawiera ona twierdzenia niezgodne ze stanem faktycznym. *** ***Poprawka 20 naniesiona na aktualne brzmienie Projektu ustawy***: „Art. 67b [...] 10. Przed wydaniem decyzji minister właściwy do spraw informatyzacji zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do Kolegium do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. ~~Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.”~~
21.	W art. 1 w pkt 76 w art. 67b w ust. 11 pkt 2 otrzymuje brzmienie: „2) potencjalnych systemowych zakłóceń dostaw i konieczności zapewnienia dywersyfikacji dostaw w przypadku blokady technologicznej;” ***Uwaga: poprawkę nr 21 należy głosować łącznie z poprawką nr 22***	Pozostawienie przesłanek z projektowanego art. 67b ust. 11 pkt 2 KSC w aktualnym kształcie może doprowadzić do uznania za DWR dostawcy, którego jedyną przewiną jest: ▪ pozostawanie pod rządami państwa spoza UE/ NATO, ▪ gdy to państwo nie zawarło z UE porozumienia dot. ochrony danych osobowych, - i to niezależnie od tego, czy dane oprogramowanie przetwarza dane osobowe. - nawet gdyby jego sprzęt nie spowodował incydentu ani nie zawierał wad (podatności). Taki skutek byłby zbyt arbitralny i mógłby doprowadzić do tego, że o uznawaniu dostawcy za DWR ostatecznie decydowałyby kwestie geopolityczne, a nie merytoryczne i autentyczna analiza ryzyka w zakresie kontroli dostępu i łańcucha dostaw. Tajemnicą poliszynela jest, że głównymi kandydatami na DWR są dostawcy z Chin.

		Warto zauważyć, że w USA nakaz usunięcia chińskiego sprzętu telekomunikacyjnego spowodował konieczność dofinansowania dla przedsiębiorców idącego w miliardy dolarów[6]. W Polsce dofinansowanie nie jest przewidziane. Brzmienie poprawki nawiązuje do motywu 90 dyrektywy NIS2 (blokada technologiczna) i nawiązuje jednego z dwóch rodzajów ryzyk, które mitygować powinna instytucja prawna DWR (ryzyko w zakresie kontroli dostępu oraz w zakresie zakłóceń łańcucha dostaw). *** ***Poprawka 20 naniesiona na aktualne brzmienie Projektu ustawy***: „Art. 67b [...] 11. Opinia, o której mowa w ust. 10 zdanie pierwsze, zawiera analizę: [...] 2) potencjalnych systemowych zakłóceń dostaw i konieczności zapewnienia dywersyfikacji dostaw w przypadku blokady technologicznej ~~prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:~~ ~~a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie,~~ ~~b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności w przypadku, gdy nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem,~~ ~~c) struktury własnościowej dostawcy sprzętu lub oprogramowania,~~ ~~d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania~~;
22.	W art. 1 w pkt 76 w art. 67b w ust. 11 po pkt. 2 dodaje się pkt. 2a i 2b w brzmieniu:	Przesłanki ujęte w proponowanym pkt 2 (poprawka nr 21) oraz przesłanka 2a to jedyne konkretne i nie całkiem arbitralne przesłanki pozatechniczne, zaczerpnięte z ostatniego zdania motywu 90 dyrektywy NIS2. Te dwie przesłanki stanowią kwintesencję problemu

[6] ttps://www.congress.gov/crs-product/IN11663

	2a) ukrytych podatności lub umyślnie stworzonych luk w produktach ICT, usługach ICT lub procesach ICT; 2b) kosztów wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT, o których mowa w ust. 16 lub 16a, oraz proporcjonalności obowiązku wycofania z użytkowania tych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT do zagrożeń podstawowego interesu bezpieczeństwa państwa, jakie mogą one powodować;" ***Uwaga: poprawkę nr 22 należy głosować łącznie z poprawką nr 21***	kwestii pozatechnicznych, przed którymi należy się bronić. W państwach członkowskich, które wdrożyły 5G Toolbox, nie ma jednej wersji przesłanek pozatechnicznych. Przesłanka 2b stanowi jednocześnie wyraz potrzeby zachowania zasady proporcjonalności. Jednym z aspektów istotnych przy ocenie proporcjonalności danego rozwiązania jest kwestia skutków finansowych danej decyzji. W aktualnym Projekcie ustawy nie przewidziano możliwości analizy skutków finansowych decyzji DWR. Przesłanka 2b służyć ma uzupełnieniu tej luki.
23.	W art. 1 w pkt 76 w art. 67c ust. 1 otrzymuje brzmienie: „1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmiot, o którym mowa w art. 67b ust. 1 nie wprowadza do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, do czasu eliminacji nadmiernej zależności od dostawcy wysokiego ryzyka przez ten podmiot. Za eliminację nadmiernej zależności od dostawcy wysokiego ryzyka uważa się obniżenie do 50% udziału sprzętu lub oprogramowania tego dostawcy w liczbie produktów ICT danego typu, usług ICT danego rodzaju i konkretnych procesów ICT stosowanych przez podmiot, o którym mowa w art. 67b ust. 1."	W 5G Toolbox mowa jest jedynie o „niezbędnych wyłączeniach" w sytuacji, gdy dany dostawca zostałby uznany za dostawcę wysokiego ryzyka. Kwestia „niezbędnych wyłączeń" nie została nigdzie zdefiniowana. W sytuacji, gdy sprzęt lub oprogramowanie pochodzą od dostawcy obciążonego większym ryzykiem, ale takiego, który nie jest powiązany z cyberatakami lub celowym powodowaniem incydentów krytycznych, wówczas zasadny może być zakaz nabywania sprzętu i oprogramowania takiego dostawcy. Jednakże nakaz wycofania z użytkowania sprawnego, funkcjonującego i bezpiecznego sprzętu nie da się pogodzić z zasadą proporcjonalności. Jednocześnie, skoro dany sprzęt i oprogramowanie jest obarczone wyższym ryzykiem, dozwolone powinno być posiadanie sprzętu DWR, jeżeli dany przedsiębiorca nie jest w pełni zależny od takiego sprzętu. *** ***Poprawka 20 naniesiona na aktualne brzmienie Projektu ustawy***: „Art. 67c. 1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o którychm mowa w art. 67b ust. 1: 1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę

		wysokiego ryzyka, **do czasu eliminacji nadmiernej zależności od dostawcy wysokiego ryzyka przez ten podmiot. Za eliminację nadmiernej zależności od dostawcy wysokiego ryzyka uważa się obniżenie do 50% udziału sprzętu lub oprogramowania tego dostawcy w liczbie produktów ICT danego typu, usług ICT danego rodzaju i konkretnych procesów ICT stosowanych przez podmiot, o którym mowa w art. 67b ust. 1.**"; 2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż w terminie 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".
24.	W art. 1 w pkt 76 w art. 67c skreśla się ust. 2, 3 i 5.	Uwzględnienie poprawki nr 23 sprawia, że projektowane art. 67c ust. 2 i 3 KSC stają się bezprzedmiotowe.
25.	W art. 1 w pkt 76 w art. 67c ust. 4 otrzymuje brzmienie: „4. Podmiot, o którym mowa w art. 67b ust. 1, do którego stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.)), nie może nabywać typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji, o której mowa w art. 67b ust. 15, do czasu eliminacji nadmiernej zależności od dostawcy wysokiego ryzyka przez ten podmiot. Za eliminację nadmiernej zależności od dostawcy wysokiego ryzyka uważa się obniżenie do 50% udziału sprzętu lub oprogramowania tego dostawcy w liczbie produktów ICT danego typu, usług ICT danego rodzaju i konkretnych procesów ICT stosowanych przez podmiot, o którym mowa w art. 67b ust. 1, do którego stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych."	Rozwiązanie analogiczne do projektowanego art. 67c ust. 1 KSC. *** ***Poprawka 20 naniesiona na aktualne brzmienie Projektu ustawy***: „Art. 67c [...] 4. Podmio~~t~~, o któr~~ych~~**m** mowa w art. 67b ust. 1, do któr~~ych~~**ego** stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.)), nie mo~~gą~~**że** nabywać typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji, o której mowa w art. 67b ust. 15**, do czasu eliminacji nadmiernej zależności od dostawcy wysokiego ryzyka przez ten podmiot. Za eliminację nadmiernej zależności od dostawcy wysokiego ryzyka uważa się obniżenie do 50% udziału sprzętu lub oprogramowania tego dostawcy w liczbie produktów ICT danego typu, usług ICT danego rodzaju i konkretnych procesów ICT stosowanych przez podmiot, o którym mowa w art. 67b ust. 1, do którego stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych**."
26.	W art. 1 w pkt 76 skreśla się art. 67d i art. 67e KSC.	W przypadku uwzględnienia poprawek nr 23-25, projektowane art. 67d i art. 67e KSC stają się bezprzedmiotowe. Jednocześnie warto dodać, że skreślenie projektowanego art. 67e

		KSC nie stoi na przeszkodzie przestrzegania przez sądy przepisów ustawy o ochronie informacji niejawnych. *** ***Poprawka 26 naniesiona na aktualne brzmienie Projektu ustawy***: ~~Art. 67d. 1. Podmioty kluczowe lub podmioty ważne są obowiązane przekazać informacje na wniosek uprawnionych organów, o których mowa w ust. 2, o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją, o której mowa w art. 67b ust. 15.~~ ~~2. Uprawnionymi organami do uzyskania informacji, o których mowa w ust. 1, są organy właściwe do spraw cyberbezpieczeństwa.~~ ~~3. Wniosek, o którym mowa w ust. 1, zawiera:~~ ~~1) wskazanie podmiotu obowiązanego do przekazania informacji;~~ ~~2) datę wydania decyzji, o której mowa w art. 67b ust. 15;~~ ~~3) wskazanie zakresu żądanych informacji;~~ ~~4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;~~ ~~5) uzasadnienie;~~ ~~6) pouczenie o zagrożeniu karą, o której mowa w art. 73.~~ ~~4. Minister właściwy do spraw informatyzacji może zwrócić się do organów właściwych do spraw cyberbezpieczeństwa, aby uzyskały informacje, o których mowa w ust. 1.~~ ~~5. Na wniosek ministra właściwego do spraw informatyzacji organ właściwy do spraw cyberbezpieczeństwa przekazuje uzyskane informacje, o których mowa w ust. 1, temu ministrowi.~~ ~~Art. 67e. 1. Sąd administracyjny rozpatruje skargę na decyzję, o której mowa w art. 67b ust. 15, na posiedzeniu niejawnym w składzie trzech sędziów.~~

		~~2. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych.~~

Załącznik nr 2 do apelu Krajowej Izby Komunikacji Ethernetowej z 2.12.2025 r. o usunięcie nadregulacji z projektu nowelizacji KSC (druk nr 1955)

dr hab. Ryszard Piotrowski
Wydział Prawa i Administracji
Uniwersytetu Warszawskiego

Warszawa 12 czerwca 2025 r.

Opinia o zgodności wybranych przepisów projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych ustaw z Konstytucją RP

Tezy opinii:

1. Art. 67 b ust. 15, w związku z art. 67 b ust. 16 i art. 67 c ust. 1 i 2, jest niezgodny z art. 2, art. 20, art. 21 ust. 2, art. 22, art. 64 w związku z art. 2 i art. 31 ust. 3 Konstytucji RP;

2. Art. 67 b ust. 2, ust. 4, ust. 10 są niezgodne z preambułą Konstytucji RP w związku z art. 2 Konstytucji RP;

3. Art. 67 e ust. 2 jest niezgodny z art. 45 ust. 2 Konstytucji RP;

4. Art. 67 g ust. 2 jest niezgodny z art. 87 ust. 1 Konstytucji RP.

Uzasadnienie:

1. W myśl art. 67 b ust. 15 projektu ustawy[1] **(dalej: projekt)** Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa. Stosownie do art. 67 b ust. 16 decyzja ministra zawiera „w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka". Skutki decyzji ministra, według art. 67 c ust. 1 projektu, polegają na

[1] Projekt z dnia 7 lutego 2025 r.

tym, że podmioty kluczowe i ważne oraz przedsiębiorcy telekomunikacyjni, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych (tak w art. 67 b ust. 1), w zakresie objętym decyzją, nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT, dostarczanych przez dostawcę wysokiego ryzyka oraz wycofują je z użytkowania nie później niż w terminie 7 lat od dnia ogłoszenia decyzji. Przedsiębiorcy telekomunikacyjni, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych, wycofują w ciągu 4 lat od dnia ogłoszenia decyzji typy produktów, rodzaje usług, konkretne procesy wskazane w decyzji. Nakaz usunięcia sprzętu lub oprogramowania nie jest podstawą do przyznania odszkodowania. Udział w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka, oprócz dostawcy będą mogli wziąć przedsiębiorcy komunikacji elektronicznej, którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa GUS (art. 67 b ust. 4). Oznacza to, że podmioty o przychodzie powyżej 10 milionów złotych, ale poniżej wskazanej dwudziestokrotności będą zobowiązane do wycofania z użytkowania sprzętu i oprogramowania wskazanych w decyzji bez możliwości udziału w przedmiotowym postępowaniu.

Niezgodność projektowanego rozwiązania z art. 2 Konstytucji RP polega na naruszeniu zakazu nadmiernej ingerencji wbrew zasadzie proporcjonalności stanowionych ograniczeń. Konsekwencją rozwoju nowych technologii jest osłabienie władzy publicznej, która nie jest w stanie zapewnić bezpieczeństwa obywatelom narażonym na konsekwencje wadliwego oprogramowania. W uzasadnieniu projektu wskazano, że „obecnie ani przedsiębiorcy

telekomunikacyjni, ani dostawcy usług zaufania nie są podmiotami krajowego systemu cyberbezpieczeństwa"2, a „państwo nie dysponuje środkami prawnymi, które umożliwiałyby skuteczną reakcję na incydent krytyczny"3 Projekt wprowadza swego rodzaju upaństwowienie podmiotów prywatnych ze względu na rodzaj działalności prowadzonej przez te podmioty, wymagającej, by państwo „mogło nakazać tym podmiotom" zachowanie, które „uchroni m. in. systemy informacyjne, sieci telekomunikacyjne wielu podmiotów przed skutkami incydentu krytycznego"4. Państwo, nie będąc w stanie chronić przed incydentem krytycznym, arbitralnie obciąża konsekwencjami tej sytuacji podmioty prywatne, obciążając je zarazem kosztami przedsięwzięcia. Nieproporcjonalność polega także na zastosowaniu środka najbardziej dolegliwego, jakim jest nakazanie wycofania z użytkowania sprzętu i oprogramowania oraz na uniemożliwieniu udziału w postępowaniu dotyczącym uznania za dostawcę wysokiego ryzyka podmiotów, które nie uzyskały wysokiego przychodu wskazanego w projekcie.

W orzecznictwie Trybunału Konstytucyjnego i w doktrynie ugruntowane jest przekonanie, że istotną część treści normatywnej art. 2 Konstytucji RP stanowi zasada zaufania obywateli do państwa i tworzonego przez nie prawa. Na tę z kolei zasadę składają się liczne, bardziej szczegółowe reguły, nazywane przez Trybunał Konstytucyjny w jego orzecznictwie "zasadami przyzwoitej legislacji"5; należy do nich zasada proporcjonalności, która – jako zasada tworzenia prawa – musi być respektowana w demokratycznym państwie prawnym. W myśl tej zasady środki zastosowane do osiągnięcia założonego przez ustawodawcę celu powinny być do tego celu proporcjonalne. Ocena proporcjonalności powinna, według Trybunału Konstytucyjnego, „udzielać odpowiedzi na trzy pytania: 1) czy wprowadzona regulacja ustawodawcza jest w

2 Por. s. 1 uzasadnienia projektu
3 Por. s. 104 uzasadnienia projektu
4 Por. s. 105 uzasadnienia projektu
5 Tak Trybunał Konstytucyjny w uzasadnieniu wyroku w sprawie o sygn. K 8/98

stanie doprowadzić do zamierzonych przez nią skutków (kryterium przydatności); 2) czy regulacja ta jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana (kryterium konieczności); 3) czy efekty wprowadzanej regulacji pozostają w proporcji do ciężarów nakładanych przez nią na obywatela (proporcjonalność sensu stricto)"6. Trybunał uznał, że art. 2 Konstytucji RP jest źródłem zasady proporcjonalności i może być wzorcem stanowiącym wyłączną podstawę kontroli konstytucyjności7. Wskazał również, ze ocena naruszenia zasady proporcjonalności przez zawarte w ustawie rozwiązania powinna być dokonywana z perspektywy efektywności regulacji, konieczności oraz stopnia dolegliwości8.

Przedmiotowa regulacja jest w stanie doprowadzić do zamierzonych skutków, ale nie jest niezbędna do ochrony interesu publicznego, ponieważ możliwe jest zastosowanie takich środków, jak certyfikacja cyberbezpieczeństwa, czy też dywersyfikacja dostawców sprzętu i oprogramowania. Ze względu na zakres i dolegliwość ingerencji należy uznać, że efekty regulacji nie pozostają w proporcji do nakładanych ciężarów.

Naruszenie zasady proporcjonalności powoduje zarazem, że opiniowana regulacja jest niezgodna z dekodowaną z zasady demokratycznego państwa prawnego zasadą racjonalności działań prawodawcy. W orzecznictwie Trybunału Konstytucyjnego wskazano, że „państwo prawne opiera się na założeniu racjonalności prawodawcy, a warunkiem koniecznym realizacji tego założenia jest przestrzeganie proporcjonalności w procesie stanowienia prawa"9. Nieproporcjonalność ustanowionej w opiniowanych przepisach kary administracyjnej powoduje zatem niezgodność tych przepisów z zasadą racjonalności działań prawodawcy.

---

6 Por. w szczególności w uzasadnieniu wyroku w sprawie o sygn. K 11/94. Por. także M. Chmaj, M. Urbaniak: Komentarz do Konstytucji RP. Art. 2. Warszawa 2022, s. 65 i nast.
7 Tak w uzasadnieniu wyroku w sprawie o sygn. P 8/10.
8 Ibidem.
9 Tak w uzasadnieniu wyroku w sprawie o sygn. K 9/98.

Według Trybunału Konstytucyjnego „podstawą każdego systemu norm prawnych jest fikcja prawna racjonalności prawodawcy"10, a jednocześnie „punktem wyjścia dla kontroli konstytucyjności prawa jest zawsze założenie racjonalnego działania ustawodawcy"11.

W orzecznictwie Trybunału Konstytucyjnego znajduje wyraz przekonanie, „że wszelkie działania prawodawcy są efektem dogłębnego rozważenia problemu i dojrzałej decyzji znajdującej racjonalne uzasadnienie. Wynika więc stąd, że stanowione prawo cechuje się założonym z góry racjonalizmem"12.

To właśnie ów racjonalizm ustawodawcy, potwierdzony w treści ustawy, pozwala wymagać respektowania prawa. Zdaniem Trybunału „odrzucenie fikcji racjonalności ustawodawcy wiązałoby się z dopuszczeniem możliwości podważania poszczególnych aktów prawnych i odmowy ich stosowania, to zaś groziłoby rozprzężeniem wszystkich więzi prawnych i społecznych. Skoro punktem wyjścia jest przyjęcie racjonalności ustawodawcy (i wynikającego stąd racjonalizmu poszczególnych unormowań prawnych), to racjonalizm stanowionego prawa musi zostać uznany za składową przyzwoitej legislacji"13, nieodzownej dla zagwarantowania zaufania obywatela do państwa i stanowionego przez nie prawa.

Niezgodność opiniowanych przepisów z zasadą racjonalności ustawodawcy jest równoznaczna z ich niezgodnością z art. 2 Konstytucji RP.

Projektowane rozwiązanie, wprowadzając swego rodzaju upaństwowienie podmiotów prywatnych przez arbitralne i nieproporcjonalne ograniczenie możliwości działania tych podmiotów, jest niezgodne z art. 20 Konstytucji RP, w myśl którego społeczna gospodarka rynkowa oparta na wolności działalności

10 Tak w uzasadnieniu wyroku w sprawie o sygn. P 6/04.
11 Tak w uzasadnieniu wyroku w sprawie o sygn. K 5/99.
12 Tak w uzasadnieniu wyroku w sprawie o sygn. P 6/04.
13 Ibidem.

gospodarczej, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych stanowi podstawę ustroju gospodarczego Rzeczypospolitej Polskiej. W orzecznictwie Trybunału Konstytucyjnego znalazł wyraz pogląd, że uczynienie własności prywatnej jedną z podstaw gospodarki rynkowej wynika z zakazu powrotu do systemu, w którym dominuje własność państwowa oraz własność podmiotów powiązanych z państwem14. W opiniowanym zakresie projektowane rozwiązanie wprowadza nadmierne niż dopuszczalne w społecznej gospodarce rynkowej powiązanie podmiotów prywatnych z państwem.

Projektowana regulacja nie przewiduje przyznania odszkodowania z tytułu usunięcia sprzętu lub oprogramowania, co jest równoznaczne z pozbawieniem własności przysługującej podmiotom zobowiązanym na mocy ustawy, a więc z wywłaszczeniem na cele publiczne. Jest to niezgodne z art. 21 ust. 2 Konstytucji, w myśl którego wywłaszczenie jest dopuszczalne, jedynie wówczas, gdy jest dokonywane na cele publiczne i za słusznym odszkodowaniem. Według Trybunału Konstytucyjnego wywłaszczenie należy rozumieć szeroko, jako przymusowe odebranie wszelkich praw majątkowych15, a wywłaszczenie może zostać dokonane także aktem generalnym16.

Opiniowane przepisy ustanawiają ograniczenie prawa własności przedsiębiorców telekomunikacyjnych, które może prowadzić nawet do rezultatów równoznacznych z pozbawieniem własności ze względu na nakaz usunięcia sprzętu lub oprogramowania bez przyznania odszkodowania.

Z orzecznictwa Trybunału Konstytucyjnego wynika, że chociaż prawo własności jest traktowane jako prawo podmiotowe o najszerszej treści, i w porównaniu z innymi prawami jako prawo najsilniejsze w stosunku do rzeczy, nie jest jednak prawem absolutnym (*ius infinitum*), a więc prawem w swojej

14 Tak w uzasadnieniu wyroku w sprawie o sygn. K 14/99.
15 Tak w uzasadnieniu wyroku w sprawie o sygn. Sk 39/15.
16 Por. P. Tuleja w: P. Tuleja, red.: Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warszawa 2019, s. 91.

treści niczym nie ograniczonym17. Trybunał stwierdził przy tym, że poręczenia całkowitej ochrony własności nie można rozumieć krańcowo, tzn. w tym sensie, że każda ingerencja ustawodawcy w sferę własności osobistej stanowi naruszenie Konstytucji, która „chroni różne dobra, zarówno związane z interesem indywidualnym obywateli, jak i potrzebami całego społeczeństwa. Stosownie do okoliczności zachodzi nieraz potrzeba dania pierwszeństwa jednym dobrom przed drugimi"18. Ograniczenie własności jest zatem dopuszczalne, jeżeli pozostaje w granicach konstytucyjnych gwarancji prawa własności. Identyfikując te gwarancje Trybunał Konstytucyjny stwierdził19, że prawo własności i jego ochronę należy konstruować na tle ogólnych zasad ustroju Rzeczypospolitej. W świetle tych zasad zagwarantowanie ochrony własności jest konstytucyjną powinnością państwa i stanowi wartość wyznaczającą kierunek interpretacji zarówno Konstytucji, jak i unormowań zawartych w ustawodawstwie zwykłym. Ochrona własności nie może mieć charakteru absolutnego. Ocena wszelkich regulacji dotyczących prawa własności nie sprowadza się więc do zagadnienia prawnej dopuszczalności wprowadzania ograniczeń jako takich, ale do kwestii dochowania konstytucyjnych ram, w jakich podlegające ochronie konstytucyjnej prawo może być ograniczane20. Ograniczenia prawa własności dopuszczalne są tylko w zakresie, w jakim nie naruszają istoty tego prawa.

Uznanie, że ograniczenia mogą być ustanawiane tylko wtedy, gdy są konieczne w demokratycznym państwie, nakazuje rozważyć: czy wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków; czy regulacja ta jest niezbędna dla ochrony interesu publicznego, z którym jest połączona; czy efekty wprowadzonej regulacji pozostają w odpowiedniej proporcji do ciężarów nakładanych przez nią na obywatela21. Jak już

17 Tak w uzasadnieniu wyroku w sprawie o sygn. P 6/92.
18 Tak w uzasadnieniu wyroku w sprawie o sygn. K 6/98.
19 Por. uzasadnienie wyroku w sprawie o sygn. P 11/98.
20 Por. uzasadnienie wyroku w sprawie o sygn. P 2/98.
21 Tak zwłaszcza w uzasadnieniu wyroku w sprawie o sygn. K 42/07.

stwierdzono w przypadku opiniowanych przepisów mamy do czynienia z naruszeniem zakazu nadmiernej ingerencji. Tym samym ustanawiane w tych przepisach ograniczenia nie są konieczne w demokratycznym państwie i z tego względu nie mogą mieć miejsca.

W świetle orzecznictwa konstytucyjnego wprowadzone w opiniowanych przepisach ograniczenia w sposobie korzystania z własności mogą zostać uznane za konstytucyjnie dopuszczalne wówczas, gdy są uzasadnione potrzebą ochrony wartości konstytucyjnych22 (dookreślają je postanowienia art. 31 ust. 3 Konstytucji oraz inne normy konstytucyjne) i są konieczne w demokratycznym państwie. Wskazuje to na potrzebę respektowania zasady proporcjonalności, według której użyte przez ustawodawcę środki powinny pozostawać w odpowiedniej proporcji do zamierzonego rezultatu23.

Art. 31 ust. 3 Konstytucji RP stanowi, że ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

W myśl art. 64 ust. 1 i 2 każdy ma prawo do własności, a także innych praw majątkowych, które podlegają równej dla wszystkich ochronie prawnej.

Stosownie do art. 2 ustawy zasadniczej Rzeczpospolita jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej.

Ograniczenia w zakresie korzystania z własności podlegają ocenie dotyczącej ich zgodności z dekodowaną z art. 2 Konstytucji RP zasadą ochrony zaufania do państwa i prawa, określaną w orzecznictwie Trybunału także jako „zasada lojalności państwa wobec adresata norm prawnych. Wyraża się ona w

22 Tak w uzasadnieniu wyroku w sprawie o sygn. SK 6/12.
23 Tak w uzasadnieniu wyroku w sprawie o sygn. K 29/06.

stanowieniu i stosowaniu prawa w taki sposób, by nie stawało się ono swoistą pułapką dla obywatela, który powinien móc układać swoje sprawy w zaufaniu, że nie naraża się na prawne skutki niedające się przewidzieć w momencie podejmowania decyzji i że jego działania są zgodne z obowiązującym prawem oraz także w przyszłości będą uznawane przez porządek prawny"24. Według Trybunału Konstytucyjnego „ogólne zasady wynikające z art. 2 Konstytucji powinny być przestrzegane szczególnie restryktywnie, gdy chodzi o akty prawne ograniczające wolności i prawa obywatelskie oraz nakładające obowiązki wobec państwa"25. W przypadku opiniowanych przepisów mamy do czynienia z nałożeniem na wskazane w nich podmioty obowiązków wobec państwa ukształtowanych w taki sposób, że prowadzenie działalności gospodarczej w tym zakresie sprowadza zagrożenie dla prawa własności; zagrożenie to ma swoje źródło we władczej ingerencji państwa spowodowanej okolicznościami, za które podmiot, którego przedmiotowe przepisy dotyczą nie ponosi odpowiedzialności.

Dopuszczalność ograniczeń prawa własności, tak samo jak wszelkich innych konstytucyjnych praw i wolności jednostki, musi być oceniana z punktu widzenia ogólnych przesłanek ustanowionych w art. 31 ust. 3 Konstytucji, w szczególności z punktu widzenia zasady proporcjonalności (zakazu nadmiernej ingerencji), która jest zarazem jedną z zasad przyzwoitej legislacji26 dekodowanych z art. 2 Konstytucji RP.

Korzystanie z własności podlega ograniczeniom przewidzianym w art. 31 ust. 3 Konstytucji RP. Ustabilizowane orzecznictwo Trybunału Konstytucyjnego określa przesłanki i model oceny konstytucyjności rozwiązań prawnych, określających sposoby rozwiązania kolizji konstytucyjnie chronionych dóbr27, w odwołaniu do postanowienia art. 31 ust. 3 Konstytucji. Przepis ten formułuje kumulatywnie ujęte przesłanki dopuszczalności ograniczeń korzystania z

24 Tak w uzasadnieniu wyroku w sprawie o sygn. K 48/04

25 Ibidem.

26 Por. L. Garlicki, Polskie prawo konstytucyjne, Warszawa 2022, s. 74 i nast.

27 Por. M. Safjan, L. Bosek, Konstytucja RP. Komentarz, Warszawa 2016, t. I, s. 801.

konstytucyjnych praw i wolności. Są to: ustawowa forma ograniczenia, istnienie w państwie demokratycznym konieczności wprowadzenia ograniczenia, funkcjonalny związek ograniczenia z realizacją wskazanych w art. 31 ust. 3 wartości (bezpieczeństwo państwa, porządek publiczny, ochrona środowiska, zdrowia i moralności publicznej, wolności i praw innych osób) oraz zakaz naruszania istoty danego prawa lub wolności. W myśl art. 64 ust. 3 Konstytucji RP własność może być ograniczona tylko w drodze ustawy i tylko w zakresie, w jakim nie narusza ona istoty prawa własności.

W orzecznictwie Trybunału Konstytucyjnego „istota" wolności i praw człowieka i obywatela rozumiana jest jako „nienaruszalny rdzeń" każdej wolności i każdego prawa. Nienaruszalność ta polega na tym, że nawet ograniczenia zgodne ze wszystkimi innymi normami konstytucyjnymi absolutnie nie mogą dotykać pewnej sfery gwarantowanych przez Konstytucję uprawnień. Sfera ta wyznaczona jest przez funkcję danej wolności lub prawa podmiotowego, określoną przy uwzględnieniu podstawowych zasad konstytucyjnych. Gdy chodzi o własność jako najważniejsze prawo objęte ochroną opartą na art. 64 Konstytucji, naruszenie jej istoty nastąpiłoby w razie, gdyby wprowadzone ograniczenia dotyczyły podstawowych uprawnień składających się na treść własności i uniemożliwiały realizowanie przez to prawo funkcji, którą ma ono spełniać w porządku prawnym opartym na założeniach wskazanych w art. 20 Konstytucji, w myśl którego podstawę ustroju gospodarczego Rzeczypospolitej stanowi społeczna gospodarka rynkowa oparta na wolności działalności gospodarczej, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych. Uprawnieniami składającymi się na treść prawa własności są „konstytucyjnie gwarantowana wolność nabywania mienia, jego zachowania oraz dysponowania nim"28. W przypadku ograniczeń prawa własności wprowadzonych przez opiniowane przepisy ma miejsce ingerencja w treść prawa własności polegająca na tym, że zostaje zagrożone

28 Tak w uzasadnieniu wyroku w sprawie o sygn. K 33/00.

prawo własności w konsekwencji podjęcia decyzji o uznaniu dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, której skutki dotykają przedsiębiorców telekomunikacyjnych w okolicznościach niezależnych od nich, co może doprowadzić do pozbawienia zainteresowanych zdolności wykonywania działalności gospodarczej, a więc zdolności zachowania mienia i dysponowania nim.

Stwierdzenie, że ograniczenia mogą być ustanawiane tylko wtedy, gdy są konieczne w demokratycznym państwie, nakazuje rozważyć: czy wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków; czy regulacja ta jest niezbędna dla ochrony interesu publicznego, z którym jest połączona; czy efekty wprowadzonej regulacji pozostają w odpowiedniej proporcji do ciężarów nakładanych przez nią na obywatela29.

W świetle orzecznictwa konstytucyjnego wprowadzone w opiniowanych przepisach ograniczenia w sposobie korzystania z własności mogą zostać uznane za konstytucyjnie dopuszczalne wówczas, gdy są uzasadnione potrzebą ochrony wartości konstytucyjnych (dookreślają je postanowienia art. 31 ust. 3 Konstytucji oraz inne normy konstytucyjne) i są konieczne w demokratycznym państwie. Wskazuje to na potrzebę respektowania zasady proporcjonalności, według której użyte przez ustawodawcę środki powinny pozostawać w odpowiedniej proporcji do zamierzonego rezultatu30. Jednakże ingerencja państwa w prawa majątkowe przedsiębiorców telekomunikacyjnych przewidziana w projekcie ze względu na nieproporcjonalność wykracza poza konstytucyjnie dopuszczalny standard ograniczania własności.

Trybunał Konstytucyjny wyraził pogląd, że wskazana w art. 31 ust. 3 Konstytucji RP "przesłanka porządku publicznego, mimo jej dalece niedookreślonego treściowo charakteru mieści w sobie niewątpliwie postulat takiego ukształtowania stanu faktycznego wewnątrz państwa, który umożliwia

29 Tak zwłaszcza w uzasadnieniu wyroku w sprawie o sygn. K 42/07.
30 Tak w uzasadnieniu wyroku w sprawie o sygn. K 29/06.

normalne współżycie jednostek w organizacji państwowej. Dokonując ograniczenia konkretnego prawa lub wolności, ustawodawca kieruje się w tym przypadku troską o należyte, harmonijne współżycie członków społeczeństwa, co obejmuje zarówno ochronę interesów poszczególnych osób, jak i określonych dóbr społecznych, w tym i mienia publicznego"31. W orzecznictwie konstytucyjnym dopuszczono ograniczenia prawa własności mające oparcie w przesłance porządku publicznego32. Uznano również, że ingerencja w celu przeciwdziałania negatywnym skutkom określonych działań na rynku pracy, komunikacji, istniejącej sieci handlowej oraz dla zaspokojenia potrzeb interesów konsumentów, służy ochronie porządku publicznego33.

Opiniowane przepisy nie znajdują jednak uzasadnienia w przesłance porządku publicznego, ponieważ naruszają stan zaufania do państwa i stanowionego przez nie prawa.

Trybunał Konstytucyjny konsekwentnie przypominał, że jego zadaniem nie jest orzekanie o merytorycznej trafności rozwiązań przyjmowanych przez ustawodawcę. Do kompetencji ustawodawcy należy bowiem stosowanie prawa odpowiadającego założonym celom politycznym i gospodarczym oraz przyjmowanie takich rozwiązań prawnych, które jego zdaniem będą najlepiej służyły realizacji tych celów. Dopiero wówczas gdy ustawodawca wyjdzie poza te ramy swobody działania i naruszy określoną zasadę lub wartość konstytucyjną, dopuszczalna jest ingerencja Trybunału34. W orzecznictwie wskazano, że ustawodawca „może nowelizować prawo także na niekorzyść obywateli, jeżeli odbywa się to w zgodzie z Konstytucją"35. Wybór najwłaściwszych wariantów legislacyjnych pozostaje „w ramach politycznej swobody działań parlamentu, za którą ponosi on odpowiedzialność przed elektoratem"36. Trybunał Konstytucyjny wielokrotnie podkreślał, że

31 Tak w uzasadnieniu wyroku w sprawie o sygn. P 2/98.
32 Tak w uzasadnieniu wyroku w sprawie o sygn. P 11/98.
33 Tak w uzasadnieniu wyroku w sprawie o sygn. K 27/00.
34 Tak zwłaszcza w uzasadnieniu wyroków w sprawach o sygn. K 39/00, K 30/01, P 10/01.
35 Tak w uzasadnieniu wyroku Trybunału Konstytucyjnego w sprawie o sygn. K 7/95.

„sprawowanie władzy ustawodawczej należy do Sejmu i Senatu. Ustawodawca posiada całkowitą swobodę w kształtowaniu treści porządku prawnego pod warunkiem, że nie narusza Konstytucji. Ocena celowości i trafności rozstrzygnięć parlamentu wykracza poza zakres kompetencji sądownictwa konstytucyjnego. Do Trybunału Konstytucyjnego należy wyłącznie kontrola zaskarżonych aktów normatywnych z punktu widzenia ich zgodności z aktami normatywnymi wyższego rzędu. Zgodnie z ustalonym orzecznictwem Trybunału, punktem wyjścia dla kontroli konstytucyjności prawa jest zawsze założenie racjonalnego działania ustawodawcy oraz domniemanie zgodności ustaw z Konstytucją. (...) Trybunał Konstytucyjny interweniuje w tych wszystkich przypadkach, gdy ustawodawca przekroczy zakres swojej swobody działania w sposób na tyle drastyczny, że naruszenie wspomnianych klauzul konstytucyjnych stanie się ewidentne"37. Pogląd ten można odnieść do opiniowanych przepisów. W przypadku opiniowanych przepisów ma miejsce naruszenie reguł konstytucyjnych. Z tego względu cele ustawodawcy, niezależnie od oceny ich zgodności z Konstytucją RP, nie mogą zostać zrealizowane w sposób konstytucyjnie akceptowalny.

Przewidziane w opiniowanych przepisach ograniczenia prawa własności wykraczają poza konstytucyjne ramy, w jakich podlegające konstytucyjnej ochronie prawo własności może być ograniczane. Przepisy te są zatem niezgodne z art. 64 w zw. z art. 31 ust. 3 Konstytucji RP.

2. Art. 67 b ust. 2, ust. 4, ust. 10 są niezgodne z preambułą Konstytucji RP w związku z art. 2 Konstytucji RP w zakresie, w jakim przepisy te przewidują, że do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, jeżeli ustawa nie stanowi inaczej, stosuje się przepisy Kodeksu postępowania administracyjnego z wyłączeniem art. 28 (pojęcie strony), art. 31 (prawa organizacji społecznej w postępowaniu), art. 51 (wezwanie do osobistego stawienia się), art. 66a (metryka sprawy) i art. 79 (prawa strony) tej ustawy. W demokratycznym państwie prawnym ograniczenie praw strony przysługujących jej na mocy ustawy jest równoznaczne z ograniczeniem prawa do prawa przysługującego podmiotom prawnym w demokratycznym państwie prawnym..

---

36 Tak zwłaszcza w uzasadnieniu wyroku Trybunału Konstytucyjnego w sprawie o sygn. K 11/06.
37 Tak w uzasadnieniu wyroku w sprawie o sygn. K 11/94 oraz K 10/97.

Rozwiązanie wprowadzone w opiniowanych przepisach ustawy jest niezgodne z ustanowioną w preambule Konstytucji zasadą rzetelności i sprawności działalności instytucji publicznych. Trybunał Konstytucyjny w swoim orzecznictwie kilkakrotnie odniósł się do relewantnej w niniejszej sprawie zasady rzetelności i sprawności działalności instytucji publicznych, stosując tę zasadę bezpośrednio jako wzorzec kontroli kwestionowanych przepisów38, jak i odwołując się do niej pośrednio, dla uzupełnienia argumentacji w zakresie zgodności oceny unormowań z innymi wzorcami wyrażonymi w części artykułowej Konstytucji39. Ustawodawca narusza tę zasadę, ponieważ tworzy rozwiązania sprowadzające immanentne ryzyko niezgodnego z Konstytucją RP ograniczania praw przedsiębiorców telekomunikacyjnych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka, a tym samym działania instytucji publicznej wbrew konstytucyjnemu nakazowi rzetelności i sprawności.

W dotychczasowym orzecznictwie Trybunału Konstytucyjnego znalazł wyraz pogląd, że stworzenie instytucji publicznej „w kształcie uniemożliwiającym jej rzetelne i sprawne działanie" narusza „zasady państwa prawnego w zakresie konstytucyjnego prawa obywateli"40. Trybunał Konstytucyjny, dokonując oceny konkretnej instytucji publicznej utworzonej ustawą41, sformułował tym samym przesłanki oceny zgodności z ustawą zasadniczą także innych instytucji publicznych, na co wyraźnie wskazano w uzasadnieniu powoływanego wyroku, a więc w szczególności instytucji publicznych służących zagwarantowaniu bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego.

Zdaniem Trybunału Konstytucyjnego „rzetelność i sprawność działania instytucji publicznych, w szczególności zaś tych instytucji, które zostały stworzone w celu realizacji i ochrony praw gwarantowanych przez Konstytucję, należy do wartości mających rangę konstytucyjną. Wynika to jasno z tekstu wstępu do Konstytucji (tzw. preambuły), w którym jako dwa główne cele ustanowienia Konstytucji wymieniono: zagwarantowanie praw obywatelskich oraz zapewnienie rzetelności i sprawności działania instytucji publicznych. (...) Przepisy, których treść nie sprzyja rzetelności lub sprawności działania instytucji mających służyć ochronie praw konstytucyjnych stanowią zarazem naruszenie tych praw, a tym samym uzasadnione jest ich uznanie za niezgodne z Konstytucją"42.

3. W myśl art. 67 e ust. 2 projektu odpis sentencji wyroku sądu administracyjnego w sprawie decyzji o uznaniu za dostawcę wysokiego ryzyka

---

38 Tak przykładowo w uzasadnieniu wyroku w sprawie o sygn. K 31/06.
39 Tak przykładowo w uzasadnieniu wyroku w sprawie o sygn. K 14/03.
40 Tak w sentencji wyroku w sprawie o sygn. K 14/03.
41 Trybunał w szczególności stwierdził niezgodność z Konstytucją przepisów ustawy z dnia 23 stycznia 2003 r. o powszechnym ubezpieczeniu w Narodowym Funduszu Zdrowia (Dz. U. z 2003 r. Nr 45, poz. 391 ze zm.).
42 Ibidem.

doręcza się skarżącemu z tą częścią uzasadnienia, która nie zawiera informacji niejawnych. Zgodnie z art. 45 ust. 2 Konstytucji dopuszczalne jest wyłączenie jawności rozprawy, a nie jawności uzasadnienia. Ponadto powołany przepis przewiduje, że wyrok ogłaszany jest publicznie. Uzasadnienie jest częścią wyroku.

4. W myśl art. 67 g ust. 2 projektu polecenie zabezpieczające wydawane przez ministra właściwego do spraw informatyzacji dotyczy nieokreślonej liczby podmiotów kluczowych i podmiotów ważnych. Jednak art. 87 ust. 1 nie zalicza poleceń ministra do źródeł prawa powszechnie obowiązującego, a więc obowiązującego te podmioty. Polecenia ministra nie są rozporządzeniami ministra. Podmioty wskazane w art. 67 g ust. 2 projektu nie są jednostkami organizacyjnie podległymi ministrowi, a zatem nie wiążą je polecenia ministra nawet, gdyby były jego zarządzeniem.

5. Z powyższych względów należy uznać tezy opinii za uzasadnione.