PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ
Karol Nawrocki

Warszawa, dnia 17 lipca 2026 r.

Trybunał Konstytucyjny
al. Jana Chrystiana Szucha 12a
00-918 Warszawa

WNIOSEK

Na podstawie art. 191 ust. 1 pkt 1 Konstytucji Rzeczypospolitej Polskiej wnoszę o zbadanie zgodności **ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) w brzmieniu nadanym ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252).**

Ustawie tej zarzucam niezgodność:

I. art. 67b ust. 1, 15 i 16 w związku z art. 67c ust. 1, 2 i 4 oraz art. 2 pkt 11k, 11l i 11m ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – z art. 2, art. 20, art. 21 ust. 2, art. 22 oraz art. 64 ust. 2 i 3 w związku z art. 2 i art. 31 ust. 3 Konstytucji;

II. art. 67e ust. 1 i 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – z art. 45 ust. 1 w związku z art. 31 ust. 3 oraz z art. 78 w związku z art. 31 ust. 3 Konstytucji;

III. art. 67b ust. 2, 6, 8, 10-13 i 17-19 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – z art. 2, art. 7, art. 51 ust. 3 oraz art. 78 w związku z art. 31 ust. 3 Konstytucji;

IV. art. 67g ust. 1, 2, 9 pkt 2, 10 i 11 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa - z art. 87 ust. 1 oraz z art. 149 ust. 1 w związku z art. 2 i art. 31 ust. 3 oraz z art. 64 ust. 2 Konstytucji;

V. art. 67g ust. 1, 3 i 4, 14 – 17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa - z art. 2, art. 7 oraz art. 78 w związku z art. 31 ust. 3 Konstytucji.

U Z A S A D N I E N I E

Ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252), zwanej dalej „nowelizacją", dokonano zmiany przepisów obowiązującej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) – zwanej dalej jako „ustawa o KSC". Celem uchwalonej przez Sejm ustawy jest kompleksowa zmiana obowiązującego w Polsce systemu zapewnienia cyberbezpieczeństwa i podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także wdrożenie do polskiego porządku prawnego dyrektywy 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, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 – zwanej dalej „dyrektywa NIS 2" tak by polskie regulacje z zakresu cyberbezpieczeństwa były spójne z rozwiązaniami przyjętymi na poziomie Unii Europejskiej. Uchwalona w dniu 23 stycznia 2026 r. nowelizacja ma charakter wdrażający przepisy dyrektywy NIS 2 do prawa polskiego, choć jednocześnie zawiera regulacje prawne wykraczające poza wymagany prawem Unii Europejskiej zakres implementacji.

Projekt nowelizacji wpłynął do Sejmu Rzeczypospolitej Polskiej w dniu 7 listopada 2025 r. i był projektem rządowym (druk sejmowy nr 1955). W dniu 17 listopada 2025 r. projekt ustawy został skierowany do pierwszego czytania na posiedzeniu Sejmu RP. W dniu 5 grudnia

2025 r. projekt został skierowany do rozpatrzenia przez Komisję Cyfryzacji, Innowacyjności i Nowoczesnych Technologii. W dniu 9 stycznia 2026 r. Komisja wniosła o uchwalenie przez Sejm projektu ustawy w brzmieniu zaproponowanym w sprawozdaniu (druk sejmowy nr 2139).

Drugie czytanie projektu ustawy odbyło się na 50. posiedzeniu Sejmu w dniu 21 stycznia 2026 r. Sejm podjął decyzję o niezwłocznym przystąpieniu do trzeciego czytania. Sejm uchwalił ustawę na 50. posiedzeniu w dniu 23 stycznia 2026 r. Za przyjęciem ustawy głosowało 407 posłów, przy 10 głosach przeciw i 17 głosach wstrzymujących się.

Senat RP, na 51. posiedzeniu w dniu 28 stycznia 2026 r., po rozpatrzeniu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw przyjął ustawę bez poprawek (druk nr 609 i 609-A).

Uchwalona ustawa w swoim podstawowym zakresie regulacyjnym dostosowuje krajowy system cyberbezpieczeństwa do nowych wymogów prawnych wynikających z przepisów europejskich, zmieniającego się otoczenia cyfrowego oraz rosnącej skali zagrożeń w cyberprzestrzeni. Zmiany w przepisach obejmują m.in. rozszerzenie katalogu podmiotów objętych obowiązkami wynikającymi z ustawy, zastąpienie dotychczasowego podziału na operatorów usług kluczowych i dostawców usług cyfrowych nową kategorią podmiotów kluczowych i podmiotów ważnych, wzmocnienie rządowego systemu reagowania na incydenty oraz doprecyzowanie ról organów państwowych odpowiedzialnych za cyberbezpieczeństwo. Ustawa została opublikowana w Dzienniku Ustaw z dnia 2 marca 2026 r. pod poz. 252. Ustawa weszła w życie w dniu 3 kwietnia 2026 r.

W ocenie Wnioskodawcy, zaskarżone przepisy ustawy o KSC zawierają nowe regulacje prawne, m.in. w postaci znajdującego się w Rozdziale 12a ustawy mechanizmu uznawania za Dostawcę Wysokiego Ryzyka, dalej jako „DWR" czy też regulacji w zakresie wydawania poleceń zabezpieczających, które mogą mieć charakter nadmiarowy i dalece wykraczający poza konstytucyjny standard przepisów regulujących oddziaływanie władzy publicznej na sposób prowadzenia działalności gospodarczej przez przedsiębiorców w tzw. podmiotach kluczowych i podmiotach ważnych z punktu widzenia bezpieczeństwa państwa lub porządku publicznego oraz na sposób dysponowania przez przedsiębiorców będących ich własnością sprzętem oraz oprogramowaniem. W świetle dotychczasowego orzecznictwa Trybunału Konstytucyjnego nie powinno budzić wątpliwości to, że istnieje prawna dopuszczalność wprowadzania w przepisach prawa powszechnie obowiązującego ograniczeń w sposobie korzystania z własności. Jest to jednak możliwe jedynie w sytuacji, gdy zachodzi oczywista

potrzeba ochrony wartości konstytucyjnych – por. wyrok TK w sprawie o sygn. SK 6/12 i jednocześnie jest to konieczne w demokratycznym państwie – por. wyrok TK w sprawie o sygn. K 29/06.

Biorąc pod uwagę szeroki zakres podmiotowy adresatów ustawy, który wynika m.in. z art. 67b ust. 1 i nast. ustawy o KSC a obejmujący podmioty kluczowe i podmioty ważne w rozumieniu Załącznika nr 1 i nr 2 do ustawy, przedsiębiorców komunikacji elektronicznej, jak i podmioty finansowe, to zaskarżona regulacja prawna oddziaływuje na szeroki krąg podmiotów (szacunki wskazują nawet na ok. 40.000 podmiotów). Stąd też weryfikacja konstytucyjności przyjętych przez ustawodawcę mechanizmów ingerencji we własność adresatów ustawy, którzy stosują sprzęt oraz oprogramowanie (produkty ICT, usługi ICT czy też oprogramowanie ICT rozumiane zgodnie z źródłem tego skrótu w języku angielskim, jako: „Information and Communication Technology", czyli szeroko rozumiane produkty związane z technologiami informacyjnymi i komunikacyjnymi), zgodnie z zakresem wskazanym w art. 67b ust. 16 ustawy o KSC, a także ograniczeń narzucanych na dostawców sprzętu oraz oprogramowania w możliwości prowadzenia przez nich działalności gospodarczej w Polsce, ma fundamentalne znaczenie dla zachowania zaufania do państwa przez obywateli i zapewnienia racjonalności uchwalanych przez organy władzy publicznej przepisów prawa.

Wprowadzenie

Opis regulacji prawnej w zakresie pojęć „procesu ICT", „produktu ICT" i „usługi ICT"

Przepisy Rozdziału 12a ustawy o KSC (art. 67a – art. 67f) wprowadzają szczególny mechanizm nadzoru rynku pozwalający organom nadzoru na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych, za dostawcę wysokiego ryzyka. Na podstawie art. 67b ust. 2 ustawy o KSC minister właściwy do spraw informatyzacji, na podstawie decyzji administracyjnej, będzie mógł uznać dostawcę „sprzętu lub oprogramowania" (produktów ICT, usług ICT lub procesów ICT) za dostawcę wysokiego ryzyka ze skutkami prawnymi opisanymi w ustawie. Sprzęt lub oprogramowanie takiego dostawcy będą musiały być wycofane z sieci lub systemów informatycznych podmiotów kluczowych lub podmiotów ważnych, a nowy sprzęt lub oprogramowanie tego dostawcy nie będzie mogło być wprowadzane do użytku na obszarze Rzeczypospolitej Polskiej w tych podmiotach, w tym również nie będzie mogło być nabywane

przez sektor publiczny w ramach zamówień publicznych. Rozwiązanie to ma na celu zapewnienie ochrony dla „podstawowego interesu bezpieczeństwa państwa".

Przepisy art. 67b ust. 15 i 16 ustawy o KSC mają następujące brzmienie:

„15. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania oraz podmioty wchodzące w skład grupy kapitałowej, w rozumieniu art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości, w ramach której funkcjonuje dostawca, za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa.

16. Decyzja, o której mowa w ust. 15, 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 wydania decyzji ministra właściwego ds. informatyzacji zostały uregulowane w art. 67c ust. 1, 2 i 4 ustawy o KSC w następującym brzmieniu:

„Art. 67c. 1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o których 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;

2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka niepóźniej niż w terminie 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".

2. Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.

4. Podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.), nie mogą nabywać typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji, o której mowa w art. 67b ust. 15.".

Jednocześnie z treści przywołanych powyżej przepisów wynika, że kluczowym ustawowym wymogiem dla treści decyzji wydawanej na podstawie art. 67b ust. 15 będzie wskazanie „typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania", który może zostać uznany za Dostawcę Wysokiego Ryzyka (DWR). Definicję pojęć: „procesu ICT", „produktu ICT" i „usługi ICT" zawierają odpowiednio przepisy art. 2 pkt 11k, 11l i 11m ustawy o KSC.

Ustawa o KSC nie definiuje samodzielnie pojęcia „sprzętu" ani „oprogramowania" używanego w art. 67b ust. 1, 15 i 16 ustawy a posługuje się za to pojęciami: „procesu ICT", „produktu ICT" i „usługi ICT" w poniżej wskazany sposób:

1) proces ICT – to proces ICT w rozumieniu art. 2 pkt 14 rozporządzenia 2019/881;
2) produkt ICT – to produkt ICT w rozumieniu art. 2 pkt 12 rozporządzenia 2019/881;
3) usługa ICT – to usługa ICT w rozumieniu art. 2 pkt 13 rozporządzenia 2019/881.

Ustawodawca posłużył się tutaj zabiegiem legislacyjnym polegającym na przepisaniu wprost treści art. 6 pkt 12, 13 i 14 Dyrektywy 2022/2555 (NIS2). Przywołane w art. 2 pkt 11k, 11l i 11m ustawy o KSC „rozporządzenie 2019/881" to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 7.06.2019, s. 15) zmienione przez Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/37 z dnia 19 grudnia 2024 r. w sprawie zmiany rozporządzenia (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa (Dz. Urz. UE L z 15.01.2025, s. 1).

Z treści art. 2 pkt 12, 13 i 14 w/w rozporządzenia 2019/881 wynika, że:

„12) „produkt ICT" oznacza element lub grupę elementów sieci lub systemów informatycznych;

13) „usługa ICT" oznacza usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych;

14) „proces ICT" oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT".

Przy czym dla ustalenia treści normatywnej pojęć: „procesu ICT", „produktu ICT" i „usługi ICT" konieczne jest odwołanie się do definicji pojęcia „sieci lub systemów informatycznych" osobno zdefiniowanych w art. 2 pkt 2 rozporządzenia 2019/881 jako: „sieci i systemy informatyczne zgodnie z definicją w art. 4 pkt 1 dyrektywy (UE) 2016/1148" w brzmieniu:

„1) „sieci i systemy informatyczne" oznaczają:

a) sieci łączności elektronicznej w rozumieniu art. 2 lit. a) dyrektywy 2002/21/WE;

b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; lub

c) dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania;"

Przywołana „dyrektywa (UE) 2016/1148" to Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.7.2016, s. 1), która z dniem 18 października 2024 r. została wprost uchylona przez art. 44 Dyrektywy 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) (Dz. Urz. UE L 333 z 27.12.2022, s. 80). Powyższe ustalenie oznacza, że polski ustawodawca odwołał się w definicji pojęć używanych w akcie normatywnym, tj. definicji „procesu ICT", „produktu ICT" i „usługi ICT" zawartej w art. 2 pkt 11k, 11l i 11m ustawy o KSC, do przepisów prawa europejskiego, które już nie obowiązują. W konsekwencji sytuację tę należy oceniać już nie jako zagadnienie polegające na ustaleniu treści normy prawnej, ale jako zagadnienie, czy norma prawna w ogóle obowiązuje. W świetle wymogu zawartego w art. 2 Konstytucji (zasada określoności prawa) przepisy prawa, które zostały uchylone nie mogą być źródłem zachowań i decyzji władczych organów władzy publicznej. Wada ta, w ocenie Prezydenta jest nienaprawialna w drodze wykładni i wymaga dokonania zmian w samej ustawie o KSC.

Mimo braku odwołania się do obowiązujących norm w prawie europejskim możliwe jest ustalenie normatywnej treści pojęć: „procesu ICT", „produktu ICT" i „usługi ICT"– poprzez odwołanie się wprost do aktualnie obowiązującego art. 6 ust. 1 pkt a) NIS2

(2022/2555), a nie do uchylonego art. 4 pkt 1 dyrektywy (UE) 2016/1148. Przepis art. 6 ust. 1 pkt a) NIS2 definiuje pojęcie „sieci i systemów informatycznych" jako:

„a) sieć łączności elektronicznej zdefiniowaną w art. 2 pkt 1 dyrektywy (UE) 2018/1972;

b) urządzenie lub grupę wzajemnie połączonych lub powiązanych urządzeń, z których co najmniej jedno, na podstawie programu, automatycznie przetwarza dane cyfrowe; lub

c) dane cyfrowe przechowywane, przetwarzane, pobierane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania".

W art. 2 pkt 1 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz. Urz. UE L 321 z 17.12.2018, s. 36) znajduje się obowiązujące na gruncie prawa Unii Europejskiej pojęcie „sieci łączności elektronicznej", które może i docelowo powinno być użyte do zrekonstruowania treści pojęć „procesu ICT", „produktu ICT" i „usługi ICT" na użytek stosowania ustawy KSC. W świetle definicji zawartej w art. 2 pkt 1 w/w Dyrektywy 2018/1972 „sieć łączności elektronicznej" oznacza:

„systemy transmisyjne, niezależnie do tego, czy opierają się na stałej infrastrukturze lub scentralizowanym zarządzaniu zasobami, oraz, w stosownych przypadkach, urządzenia przełączające lub routingowe oraz inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają przekazywanie sygnałów przewodowo, za pomocą radia, środków optycznych lub innych rozwiązań wykorzystujących fale, w tym sieci satelitarnych, stacjonarnych (komutowanych i pakietowych, w tym internetu) i sieci ruchomych, elektroenergetycznych systemów kablowych, w zakresie, w jakim są one wykorzystywane do przekazywania sygnałów, w sieciach nadawania radiowego i telewizyjnego oraz sieciach telewizji kablowej, niezależnie od rodzaju przekazywanej informacji."

Dopiero zrekonstruowana w oparciu o kompleks przepisów Unii Europejskiej treść pojęcia „proces ICT" (art. 2 pkt 11k ustawy o KSC), będącego podstawą dla wydawania decyzji w oparciu o art. 67b ust. 15 ustawy o KSC, umożliwia dokładne wskazanie przedmiotowego zakresu zaskarżonej regulacji prawnej. Na potrzeby niniejszego wniosku i jego uzasadnienia „proces ICT" oznaczać będzie **„element lub grupę elementów sieci lub systemów informatycznych"** rozumianych jako:

a) sieć łączności elektronicznej, gdzie pojęcie to zdefiniowane w art. 2 pkt 1 dyrektywy (UE) 2018/1972 oznacza:

- systemy transmisyjne, niezależnie do tego, czy opierają się na stałej infrastrukturze lub scentralizowanym zarządzaniu zasobami, oraz, w stosownych przypadkach,
- urządzenia przełączające lub routingowe oraz
- inne zasoby, w tym nieaktywne elementy sieci,

które umożliwiają przekazywanie sygnałów przewodowo, za pomocą radia, środków optycznych lub innych rozwiązań wykorzystujących fale, w tym sieci satelitarnych, stacjonarnych (komutowanych i pakietowych, w tym Internetu) i sieci ruchomych, elektroenergetycznych systemów kablowych, w zakresie, w jakim są one wykorzystywane do przekazywania sygnałów, w:

- sieciach nadawania radiowego i telewizyjnego oraz
- sieciach telewizji kablowej,

niezależnie od rodzaju przekazywanej informacji;

b) urządzenie lub grupę wzajemnie połączonych lub powiązanych urządzeń, z których co najmniej jedno, na podstawie programu, automatycznie przetwarza dane cyfrowe; lub

c) dane cyfrowe przechowywane, przetwarzane, pobierane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania.

Tak ustalona treść normatywna pojęcia „procesu ICT" umożliwia w konsekwencji ustalenie treści pojęć: „produkt ICT" (art. 2 pkt 11l ustawy o KSC po nowelizacji), który w rozumieniu art. 2 pkt 12 rozporządzenia 2019/881 oznacza „usługę polegającą w pełni lub głównie na przekazywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych" oraz „usługi ICT (art. 2 pkt 11m ustawy o KSC po nowelizacji), która w rozumieniu art. 2 pkt 13 rozporządzenia 2019/881 oznacza „zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT".

Zarzut nr 1

Niezgodność art. 67b ust. 1, 15 i 16 w związku art. 67c ust. 1, 2 i 4 oraz art. 2 pkt 11k, 11l i 11m ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) dodanego ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252) – z art. 2, art. 20, art. 21 ust. 2, art. 22 oraz 64 ust. 2 i 3 w związku z art. 2 i art. 31 ust. 3 Konstytucji w zakresie w jakim decyzja o uznaniu podmiotu za dostawcę

wysokiego ryzyka wydawana przez ministra właściwego do spraw informatyzacji podejmowana jest w oparciu o ogólne i bliżej nie sprecyzowane kryteria oceny zawarte w klauzuli „podstawowego interesu bezpieczeństwa państwa" bez powiązania ich z zawartymi w art. 67b ust. 1 ustawy kryteriami wszczęcia postępowania administracyjnego oraz wynikami analizy zgodnie z zawartymi w art. 67b ust. 11 i 12 ustawy kryteriami analizy podmiotu będącego dostawcą sprzętu lub oprogramowania przez co zaskarżone przepisy umożliwiają wydanie decyzji o wykluczeniu dostawcy uznanego za dostawcę wysokiego ryzyka z naruszeniem konstytucyjnych zasad legalności oraz proporcjonalności. Prowadzi to do naruszenia nakazu równego traktowania przedsiębiorców poprzez zastosowanie środka prawnego w postaci eliminacji określonych podmiotów z rynku podmiotów publicznych, bez poszukiwania jakichkolwiek innych możliwych rozwiązań usuwających cyberzagrożenia, zgodnie z zasadą proporcjonalności oraz bez zapewnienia jakiejkolwiek rekompensaty z tytułu wydanej decyzji zarówno dla jej adresata, jak i dla podmiotów korzystających ze sprzętu lub oprogramowania dostarczonego wcześniej przez podmiot uznany za dostawcę wysokiego ryzyka.

Tak jak to już zostało wskazane we wprowadzeniu do wniosku przepisy Rozdziału 12a ustawy o KSC (art. 67a – art. 67f) wprowadzają szczególny mechanizm nadzoru nad rynkiem pozwalający organom nadzoru na uznanie określonego dostawcy sprzętu lub oprogramowania ICT dla podmiotów kluczowych i ważnych w rozumieniu Załącznika nr 1 i 2 do ustawy o KSC, za dostawcę wysokiego ryzyka (DWR). Kluczowym elementem analizowanych przepisów ustawy o KSC jest właśnie wprowadzenie administracyjnej procedury eliminowania z rynku podmiotów publicznych „sprzętu lub oprogramowania" pochodzącego od tzw. „dostawcy wysokiego ryzyka" dla podmiotów kluczowych i ważnych wskazanych w Załącznikach nr 1 i 2 do ustawy o KSC. Przepisy te powinny być przeanalizowane w kontekście wymogu istnienia interesu publicznego we wprowadzeniu przedmiotowych ograniczeń (art. 22 Konstytucji) oraz wymogu proporcjonalności tych ograniczeń w świetle art. 31 ust. 3 Konstytucji. Ponadto przepisy te powinny zostać zbadane pod kątem możliwego naruszenia własności (art. 64 ust. 2 Konstytucji), zasad jej dopuszczalnego ograniczania (art. 64 ust. 3 i art. 31 ust. 3 zd. 2 Konstytucji) oraz zasad słusznego odszkodowania w przypadku wywłaszczeń dokonywanych na cele publiczne (art. 21 ust. 2 Konstytucji).

Eliminacja „sprzętu lub oprogramowania" (w rozumieniu technologii informatycznych i telekomunikacyjnych zdefiniowanych jako produkty ICT, usługi ICT lub procesy ICT) z

rynku lub ograniczenie dostępu do zamówień ze strony sektora publicznego w drodze decyzji administracyjnej od strony ekonomicznej oznacza dla dostawcy stratę w postaci braku możliwości osiągania przychodu ze sprzedaży posiadanych dóbr lub usług klientom na rynku. Niezależnie bowiem od aspektów terminologicznych czy technologicznych wydanie przez właściwy organ decyzji o uznaniu konkretnego, imiennie wskazanego w decyzji dostawcy za DWR oznacza odebranie temu podmiotowi możliwości prowadzenia określonego rodzaju działalności gospodarczej w Polsce oraz publiczne napiętnowanie jako mało wiarygodnego dostawcy. Z tego punktu widzenia kluczowe znaczenie dla zbadania konstytucyjności zaskarżonych przepisów ma wskazanie odpowiedniego standardu postępowania ustawodawcy, który wprowadza ograniczenia w prowadzeniu działalności gospodarczej oraz ograniczenia w dysponowaniu własnością dla dostawców produktów ICT, usług ICT lub procesów ICT.

Na podstawie przepisów art. 67b ust. 1, 15 i 16 oraz art. 67c ust. 1, 2 i 4 ustawy o KSC minister właściwy do spraw informatyzacji, w drodze decyzji administracyjnej, będzie mógł uznać dostawcę „sprzętu lub oprogramowania" za dostawcę wysokiego ryzyka (DWR). Sprzęt lub oprogramowanie takiego dostawcy będą musiały być wycofane z sieci lub systemów informatycznych podmiotów kluczowych lub podmiotów ważnych w rozumieniu Załącznika 1 i 2 do ustawy o KSC we wskazanym terminie, a nowy sprzęt lub oprogramowanie tego dostawcy nie będzie mogło być wprowadzane do użytku na obszarze Rzeczypospolitej Polskiej, w tym nie będzie mogło być nabywane przez sektor publiczny (podmioty kluczowe oraz ważne) w ramach zamówień publicznych. Uprawnienia ministra właściwego do spraw informatyzacji mają charakter władczy względem wszystkich podmiotów dostarczających na polski rynek „sprzęt lub oprogramowanie". Przesądza o tym treść art. 67b ust. 15 ustawy o KSC, który nakazuje ministrowi takie zachowanie poprzez sformułowanie „w drodze decyzji" oraz przepis art. 67b ust. 2 ustawy o KSC wskazujący, że: *„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. 79a tej ustawy."*.

W ocenie wnioskodawcy mechanizm prawny polegający na wyposażeniu organu administracji rządowej szczebla centralnego w możliwość wycofywania z rynku produktów lub rzeczy, które mogą zagrażać życiu, zdrowiu lub szkodzić w inny sposób użytkownikom bądź innym podmiotom sam w sobie nie może być oceniany jako niedopuszczalny do ustanowienia w systemie prawnym. Przy czym analizowana sytuacja nie dotyczy sytuacji typowej dla prawa

cywilnego (odpowiedzialności deliktowej), gdzie kto z winy swojej wyrządził drugiemu szkodę obowiązany jest do jej naprawienia (art. 415 K.c.), ale sytuacji nieadekwatnej ingerencji ustawodawcy w wolność działalności gospodarczej przewidzianą w art. 22 Konstytucji. Na gruncie art. 22 Konstytucji swoboda prowadzenia działalności gospodarczej rozumiana jest jako prawo podmiotowe umożliwiające samodzielne podjęcie decyzji o podjęciu działalności gospodarczej, formie jej prowadzenia i przedmiocie zarobkowania, co wyraźnie też podkreśla art. 2 Prawa przedsiębiorców wskazujący, że: „*Podejmowanie, wykonywanie i zakończenie działalności gospodarczej jest wolne dla każdego na równych prawach.*" i co uzupełnia art. 8 Prawa przedsiębiorców wskazujący, że: „*Przedsiębiorca może podejmować wszelkie działania, z wyjątkiem tych, których zakazują przepisy prawa. Przedsiębiorca może być obowiązany do określonego zachowania tylko na podstawie przepisów prawa.*". Tak opisane publiczne prawo podmiotowe obejmujące swobodę prowadzenia i wykonywania działalności gospodarczej na gruncie art. 22 Konstytucji może być ograniczane „*tylko w drodze ustawy i tylko ze względu na ważny interes publiczny*". Trybunał Konstytucyjny wypowiadając się na temat znaczenia przepisu art. 22 Konstytucji podnosił, że: „*Przepis ten, uzupełniając treść art. 20 Konstytucji tworzy podstawy ustroju gospodarczego Polski (...) „użycie w art. 20 i 22 Konstytucji zwrotu <wolność działalności gospodarczej> świadczy wyraźnie o tym, że przepisy te można uważać także za podstawę prawa podmiotowego o randze konstytucyjnej, a nie tylko i wyłącznie za normę prawa w znaczeniu przedmiotowym i zasadę ustroju państwa*" – por. wyrok TK z dnia 7 maja 2001 r., sygn. K 19/00, wyrok TK z dnia 14 czerwca 2004 r., sygn. SK 21/03 oraz wyrok TK z dnia 29 kwietnia 2003 r., sygn. SK 24/02.

Przyjęcie zatem założenia, że swoboda prowadzenia działalności gospodarczej w Polsce ma charakter „prawa podmiotowego o randze konstytucyjnej" prowadzi do wskazania konstytucyjnego wzorca oceny analizowanych przepisów jakimi są nie tylko art. 20 i 22 Konstytucji, ale także wskazane już wcześniej art. 64 ust. 2 Konstytucji statuujący zasadę równej ochrony własności oraz art. 64 ust. 3 i art. 31 ust. 3 zd. 2 Konstytucji ustanawiające zakaz naruszania istoty prawa własności przy uwzględnieniu zasady słusznego odszkodowania obowiązującej w przypadku wywłaszczeń dokonywanych na cele publiczne (art. 21 ust. 2 Konstytucji). Na gruncie konstytucyjnej aksjologii uprawniony jest bowiem wniosek, że przepisy przewidujące możliwość orzeczenia całkowitego zakazu prowadzenia działalności gospodarczej wydane wobec konkretnego podmiotu prawa mogą i powinny być oceniane w świetle wymogów Konstytucji stawianych przepisom o wywłaszczeniu. Wywłaszczenie w znaczeniu konstytucyjnym powinno być ujmowane szeroko, jako „*wszelkie pozbawienie*

własności (...) bez względu na formę" czy też jako „*wszelkie ograniczenie bądź pozbawienie przysługującego podmiotowi prawa przez władzę publiczną*" – por. wyrok TK z dnia 21 czerwca 2005 r., sygn. P 25/02 (OTK-A 2005/6/65).

Przywołane już wcześniej przepisy art. 67b ust. 1, 15 i 16 oraz art. 67c ust. 1, 2 i 4 ustawy o KSC, w ocenie wnioskodawcy, powinny być analizowane w kontekście przywołanych powyżej przepisów Konstytucji regulujących zasady ingerencji władzy publicznej w swobodę działalności gospodarczej oraz zasady władczego pozbawienia własności na cele publiczne, gdyż w sposób nie budzący wątpliwości, co do ich treści, zawierają one postanowienia wskazujące na ingerencję w prawo swobody prowadzenia działalności gospodarczej oraz prawo własności podmiotów użytkujących sprzęt lub oprogramowanie pochodzące od dostawcy uznanego za DWR. Z uwagi na przyjęte w ustawie o KSC rozwiązania prawne ingerencja ustawodawcy dotyczy zarówno eliminacji samego dostawcy z rynku polskiego (art. 67b ust. 1, 15 i 16 ustawy o KSC), jak i eliminacji z rynku jego produktów, jeśli zostały już wprowadzone na rynek (art. 67c ust. 1 pkt 1 i 2 oraz ust. 2 ustawy o KSC), jak też pozbawia dostawcę możliwości oferowania swoich produktów podmiotom, które zobowiązane są do stosowania zakupów w trybie i na zasadach opisanych w Prawie zamówień publicznych (art. 67c ust. 4 ustawy o KSC). Przy czym decyzja organu wydawana jest z rygorem natychmiastowej wykonalności (art. 67b ust. 18 ustawy o KSC).

Należy podkreślić, że pozbawienie własności, a dokładnie pozbawienie posiadanego przez dostawcę sprzętu lub oprogramowania cech zbywalności na rynku przez władzę publiczną (na mocy decyzji administracyjnej organu), aby mogło być uznane za zgodne z wymaganiami art. 21 ust. 2 Konstytucji oraz z wymogami prawa międzynarodowego musi spełniać warunek celowości (pozbawienie prawa następuje w interesie publicznym), legalności (ingerencja musi odbywać się na warunkach określonych w ustawie) oraz proporcjonalności (musi istnieć rozsądna proporcja między środkiem i celem, do którego się dąży). Ocena zaskarżonych przepisów powinna nastąpić odrębnie w każdym z tych aspektów (kryteriów oceny).

Przed przystąpieniem do szczegółowej analizy zaskarżonych przepisów konieczne jest podkreślenie, że w świetle obowiązującego prawa, w tym i na gruncie ustawy o KSC, działalność gospodarcza polegająca na dostawie (wprowadzeniu do obrotu) sprzętu lub oprogramowania w postaci produktów ICT, usług ICT lub procesów ICT w rozumieniu art. 2

pkt 11k, 11l i 11m ustawy o KSC nie podlega co do zasady ani licencjonowaniu, ani też koncesjonowaniu. Kwestia koncesjonowania działalności gospodarczej polegającej na produkcji i dostarczaniu sprzętu lub oprogramowania w postaci produktów ICT, usług ICT lub procesów ICT może zaistnieć jedynie w sytuacji, jeśli będzie możliwe uznanie ich za „technologię o przeznaczeniu wojskowym lub policyjnym" bądź za „wyroby o przeznaczeniu wojskowym lub policyjnym" w rozumieniu art. 3 pkt 12 i 13 ustawy z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz. U. z 2023 r. poz. 1743). Z mocy bowiem art. 7 ust. 1 tej ustawy „wytwarzanie i obrót" takimi technologiami wymaga uzyskania koncesji od ministra właściwego do spraw wewnętrznych. Ustawa o KSC, w wersji obowiązującej od dnia 3 kwietnia 2026 r. nie zawiera jednak wymogu uzyskania koncesji czy też licencji na wytwarzanie i obrót w Polsce technologiami ICT, o ile nie mają one przeznaczenia wojskowego lub policyjnego.

Brak wymogu posiadania koncesji dla producentów i dystrybutorów sprzętu lub oprogramowania ICT powinien być zatem rozumiany jako wyraz przekonania ustawodawcy na dzień uchwalenia ustawy w 2018 r. a także w 2026 r. podczas dokonywania dużej nowelizacji zaskarżonej ustawy, że nie występują obiektywnie istniejące przesłanki, które nakazywałyby ustawodawcy wprowadzenie szczególnego rodzaju nadzoru nad rynkiem w/w sprzętu i oprogramowania, np. w postaci wprowadzenia wymogu posiadania licencji bądź koncesji na sprzedaż produktów ICT na wzór innych rynków regulowanych takich jak np. obrót farmaceutykami. Z tego punktu widzenia uchwalona w dniu 23 stycznia 2026 r. ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. 252) jest wyrazem zmiany podejścia ustawodawcy do kwestii nadzoru publicznego nad technologiami ICT. Po części jest to konsekwencja wdrożenia NIS2 do polskiego porządku prawnego, choć akurat wprowadzona do ustawy (Rozdział 12a i przepisy art. 67b – art. 67f ustawy o KSC) instytucja dostawcy wysokiego ryzyka nie wynika wprost z przepisów NIS2 a jest jedynie wynikiem wydanej przez Komisję Europejską rekomendacji w zakresie tzw. „5G-ToolBox" opublikowanej w styczniu 2020 r. a stosowanej jedynie w odniesieniu do technologii 5G.[1] Przewodnik „5G-ToolBox" nie ma przy tym charakteru obligatoryjnego w stosowaniu przez Państwa członkowskie UE a jest zestawem dobrych praktyk i dotyczy sektora telekomunikacyjnego jedynie w części dotyczącej użytkowania technologii 5G. Jak wskazali

[1] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

sami autorzy tego przewodnika w jego pkt 2: „Celem niniejszego zestawu wsparcia jest określenie możliwego wspólnego zestawu narzędzi, które będą mogły ograniczyć zasadnicze cyberzagrożenia dla sieci 5G, zgodnie z tymi ryzykami, które zostały zidentyfikowane w sprawozdaniu ze skoordynowanej oceny ryzyka UE, oraz dostarczenie takich wskazówek dotyczących wyboru narzędzi, które powinny być traktowane priorytetowo w planach zmniejszania ryzyka cyberzagrożeń na poziomie krajowym i unijnym. Ma to na celu stworzenie solidnych ram działania mających na celu zapewnienie odpowiedniego poziomu cyberbezpieczeństwa w sieciach 5G na terenie całej UE oraz skoordynowanego podejścia pomiędzy państwami członkowskimi". Oznacza to, że kategoria prawna „dostawcy wysokiego ryzyka" nie może być identyfikowana jako element wdrażający prawo europejskie, tj. NIS2, ale jest samodzielnym działaniem ustawodawcy polskiego, który poszukując rozwiązań prawnych umożliwiających mu realny wpływ i kontrolę nad rynkiem technologii informatycznych oraz telekomunikacyjnych ustanowił mechanizm identyfikacji dostawcy wysokiego ryzyka oraz jego eliminacji (ograniczenia dostępności) z rynku oraz oferowanych przez niego produktów. Innych mechanizmów eliminacji lub ograniczania cyberzagrożeń w odniesieniu do dostawców sprzętu lub oprogramowania ustawodawca nie przewidział. Należy podkreślić, że sama instytucja dostawcy wysokiego ryzyka oparta jest na kryterium podmiotowym, na co wskazuje sformułowanie „dostawca ten" użyte w art. 67b ust. 15 ustawy o KSC, a nie na kryterium przedmiotowym, tj. występowania luk technicznych lub innego typu wad sprzętu lub oprogramowania, których występowanie zagraża „podstawowemu interesowi bezpieczeństwa państwa" wskutek generowania incydentów naruszających cyberbezpieczeństwo. Kwestia ta będzie jeszcze analizowana poniżej w związku z treścią przepisów art. 67b ust. 10-12 ustawy o KSC. Ustawodawca nie zdecydował się też np. na wprowadzenie obowiązku licencjonowania lub koncesjonowania dla dostawców sprzętu lub oprogramowania ICT dla sektora publicznego lub innych mechanizmów monitorowania, naprawiania luk sprzętu lub oprogramowania ICT oraz usuwania różnego poziomu ryzyk.

Biorąc pod uwagę to, że konstytucyjnym wymogiem dla wprowadzania regulacji prawnych ograniczających wolność gospodarczą jest istnienie interesu publicznego, to zadaniem ustawodawcy w toku procesu legislacyjnego jest takie formułowanie zakazów podejmowania lub wykonywania określonych czynności w ramach działalności gospodarczej, które w konsekwencji będą służyły interesowi publicznemu – argument z art. 22 Konstytucji. W przypadku analizowanej ustawy o KSC, w wersji obowiązującej od dnia 3 kwietnia 2026 r. interes publiczny rozumiany jest przez ustawodawcę jako „podstawowy interes bezpieczeństwa

państwa" (art. 67b ust. 15 ustawy o KSC). Pojęcie to nie zostało na gruncie ustawy zdefiniowane i zostało użyte jeszcze tylko raz w całej ustawy o KSC w art. 59b ust. 3 pkt 3 jako jedna z przesłanek odmowy udzielenia pomocy przez organ właściwy ds. cyberbezpieczeństwa organom innych państw członkowskich Unii Europejskiej w sprawowaniu nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi, których systemy informacyjne znajdują się na terytorium Rzeczypospolitej Polskiej.

Analiza semantyczna pojęcia „podstawowy interes bezpieczeństwa państwa" wskazuje, że jest to szczególna, kwalifikowana forma klauzuli generalnej „bezpieczeństwa państwa", którą posługuje się ustawodawca m.in. w art. 126 ust. 2 czy art. 146 ust. 4 Konstytucji. Na gruncie tych przepisów, bezpieczeństwo państwa jest utożsamiane z bezpieczeństwem narodowym, obejmującym suwerenność państwową, integralność terytorialną, a także stabilność struktur państwowych. Klauzula ta obejmuje swoim zakresem ochronę przed zagrożeniami militarnymi i niemilitarnymi, zarówno zewnętrznymi, jak i wewnętrznymi. Jej zasadniczym elementem jest adresowany do władz publicznych nakaz podejmowania niezbędnych działań w celu ochrony porządku publicznego i zapewnienia ciągłości funkcjonowania instytucji państwowych. Bezpieczeństwo państwa zostało też wymienione w art. 31 ust. 3 Konstytucji jako jedna z przesłanek ograniczeń praw i wolności jednostki, co wynika z użytego sformułowania „gdy [ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw] są konieczne w demokratycznym państwie dla jego bezpieczeństwa". Jak orzekł Trybunał Konstytucyjny w wyroku z dnia 25 listopada 2003 r., sygn. akt K 37/02, *„jeden z zasadniczych celów Rzeczypospolitej Polskiej jakim jest ochrona niepodległości i nienaruszalności jej terytorium uzasadnia wprowadzenie ograniczeń w wykonywaniu konstytucyjnych praw i wolności służących jednostkom*". Jasne jest zatem, że ze względu na potrzebę zapewnienia „bezpieczeństwa państwa" i celem usunięcia istniejących bądź potencjalnych zagrożeń władze publiczne mogą wprowadzać niezbędne ograniczenia praw i wolności. Z uwagi na to, że utrzymanie stanu bezpieczeństwa wewnętrznego i zewnętrznego jest, zgodnie z art. 146 ust. 4 pkt 7 i 8 Konstytucji zadaniem Rady Ministrów, to przypisanie ministrowi właściwemu do spraw informatyzacji kompetencji do ograniczania konstytucyjnych wolności i praw, zdaniem wnioskodawcy, mieści się zasadniczo w konstytucyjnym domniemaniu kompetencji Rady Ministrów do zarządzania bieżącymi sprawami państwa, w tym i w obszarze cyberbezpieczeństwa zgodnie z zakresem przedmiotowym analizowanej ustawy o KSC.

Mając zatem na względzie konstytucyjne znaczenie klauzuli generalnej „bezpieczeństwa państwa" możliwe jest wskazanie, że pojęcie „podstawowego interesu bezpieczeństwa państwa" powinno być rozumiane jako pewna forma zawężenia pojęcia „bezpieczeństwa państwa" jedynie do kwestii zasadniczych i umożliwiająca ochronę fundamentalnych interesów państwa oznaczonych jako „podstawowy interes". W tym kontekście, organ stosujący przepis art. 67b ust. 15 ustawy o KSC obowiązany będzie do zastosowania selekcji dostawców sprzętu lub oprogramowania ICT i oceny tego czy będą oni stanowili zagrożenie nie tylko militarne bądź niemilitarne, ale także czy samo to zagrożenie stanowi zagrożenie dla „podstawowych interesów" Rzeczypospolitej Polskiej bez względu na jego postać. Należy podkreślić, że ustawodawca nie posługuje się w art. 67b ust. 15 i 16 ustawy o KSC pojęciem „cyberzagrożenia" w rozumieniu art. 2 pkt 8 ustawy o KSC, ale ujmuje pojęcie zagrożenia szeroko, nie wykluczając, wszakże kategorii cyberzagrożeń. W tym kontekście, odwołanie się przez ustawodawcę do klauzuli „podstawowego interesu bezpieczeństwa państwa" przy możliwości eliminacji z rynku dostawców uznanych za zagrożenie mieści się w szeroko rozumianym warunku celowości wynikającym z art. 21 ust. 2 Konstytucji. Zapewnienie ochrony bezpieczeństwa państwa jest niewątpliwie zadaniem rządu i jednym z podstawowych celów jego działania, co wprost wynika z art. 146 ust. 4 pkt 7 i 8 Konstytucji.

Powyższa analiza musi zostać uzupełniona o wskazanie rozbieżności terminologicznej zawartej w samym art. 67b ustawy o KSC, a która w ocenie wnioskodawcy, może mieć wpływ na wynik oceny konstytucyjności zaskarżonych przepisów. Tak jak to już zostało wskazane powyżej, decyzja o uznaniu konkretnego podmiotu (przedsiębiorcy) za dostawcę wysokiego ryzyka wydawana na podstawie art. 67b ust. 15 ustawy o KSC uzależniona jest od ustalenia w toku postępowania administracyjnego czy podmiot ten „stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa". Jednocześnie samo wszczęcie postępowania administracyjnego warunkowane jest ustaleniem przez organ z urzędu lub na wniosek zaistnienia potrzeby „ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego" (art. 67b ust. 1 zdanie pierwsze ustawy o KSC). Jakkolwiek pojęcia te są znaczeniowo zbliżone do siebie, gdyż oparte są one o pojęcie „bezpieczeństwa", o tyle ich zakresy nie pokrywają się w pełni ze sobą. W konsekwencji w obrębie jednej jednostki redakcyjnej (art. 67b ustawy o KSC) istnieje rozbieżność pomiędzy przesłankami wszczęcia postępowania administracyjnego a przesłanką wydania decyzji rozstrzygającej o eliminacji dostawcy z rynku, a co w ocenie wnioskodawcy może być podstawą do postawienia zarzutu o braku dochowania przez ustawodawcę wymogu zachowania należytej staranności przy

tworzeniu prawa według którego ma działać organ, który w władczy sposób decyduje o prawach i wolnościach podmiotu prawa, tj. naruszenie art. 2 Konstytucji.

Należy też wskazać, że dotychczas Trybunał Konstytucyjny konsekwentnie stał na stanowisku, że z konstytucyjnej zasady państwa prawnego (art. 2 Konstytucji) wynika nakaz przestrzegania przez ustawodawcę zasad poprawnej legislacji, który jest funkcjonalnie związany z zasadami pewności i bezpieczeństwa prawnego oraz ochrony zaufania do państwa i prawa. Jak stwierdził Trybunał Konstytucyjny w wyroku z dnia 14 czerwca 2000 r., sygn. P 3/00, zasada zaufania do państwa i stanowionego przez nie prawa „*opiera się na wymaganiu pewności prawa, a więc takim zespole cech przysługujących prawu, które zapewniają jednostce bezpieczeństwo prawne; umożliwiają jej decydowanie o swoim postępowaniu na podstawie pełnej znajomości przesłanek działania organów państwowych oraz konsekwencji prawnych, jakie jej działania mogą pociągnąć za sobą*". Szczególne znaczenie ma ta zasada dla obrotu gospodarczego, czyli dla przedsiębiorców, którzy uczestnicząc w wymianie handlowej dóbr i usług, kalkulują ryzyka prawne i ekonomiczne związane z realizacją kontraktów. Podejmowane względem przedsiębiorców działania ze strony organów władzy publicznej zmierzające do usunięcia konkretnych dostawców dóbr i usług lub ich produktów muszą opierać się o z góry znane kryteria oceny i przesłanki podejmowania decyzji o charakterze władczym. Wskazana powyżej rozbieżność pomiędzy przesłanką wszczęcia postępowania administracyjnego a przesłanką orzekania przez organ może prowadzić do wydawania rozstrzygnięć w oparciu o niejasne kryteria oceny, których wzruszenie nie będzie możliwe w toku kontroli instancyjnej, gdyż ta z mocy art. 67b ust. 19 ustawy o KSC została wyłączona. Ponadto, wydawana w trybie art. 67b ust. 15 ustawy o KSC decyzja podlega też *ex lege* natychmiastowemu wykonaniu (art. 67b ust. 18 ustawy o KSC), co oznacza, że istnieje duże prawdopodobieństwo wyrządzenia szkody adresatowi decyzji na skutek jej wykonania, bez względu na wynik ewentualnego postępowania sądowego badającego legalność wydanej decyzji.

Drugim warunkiem konstytucyjności regulacji prawnej odnoszącej się do zagadnień odjęcia własności jest ocena tego czy opisana w ustawie władcza ingerencja organu odbywa się na warunkach określonych w ustawie, tj. czy przepisy badanego aktu normatywnego (art. 67b ust. 15 ustawy o KSC) zawierają jasne i czytelne kryteria oceny producenta bądź dostawcy sprzętu lub oprogramowania ICT pod kątem stopnia jego ryzyka dla podstawowego interesu bezpieczeństwa państwa oraz czy analizowana regulacja zawiera niezbędne gwarancje proceduralne dla podmiotu będącego adresatem decyzji, chroniące go przed arbitralnością

postępowania i podejmowanych rozstrzygnięć. Legalność przesłanek pozbawienia możliwości prowadzenia działalności gospodarczej i w konsekwencji odjęcia lub ograniczenia własności w rozumieniu konstytucyjnym oznacza nie tylko na przyjęciu samej regulacji prawnej w postaci ustawy, jako aktu normatywnego o mocy powszechnie obowiązującej, ale przede wszystkim na wprowadzeniu do takiej ustawy normatywnych kryteriów oceny, przy pomocy których organ wydający decyzję administracyjną ma ustalić okoliczności istotne dla rozstrzygnięcia sprawy. Biorąc pod uwagę treść kluczowego dla niniejszej sprawy przepisu art. 67b ust. 15 ustawy o KSC, to ustawodawca posługuje się w nim tylko jednym kryterium zagrożenia dla podstawowego interesu bezpieczeństwa państwa, jaki wiąże się z konkretnym dostawcą sprzętu lub oprogramowania. Takie ujęcie kryterium oceny dostawców za DWR pozostawia orzekającemu organowi daleko idącą swobodę decydowania, o tym, co stanowi zagrożenie a co nie. W tym miejscu trzeba podkreślić, że ustawodawca nie uzależnił wydania decyzji od zidentyfikowania chociażby cyberzagrożenia w rozumieniu art. 2 pkt 4a ustawy o KSC, który odsyła do definicji zawartej w art. 2 pkt 8 rozporządzenia 2019/881 a który to przepis definiuje „cyberzagrożenie" jako „wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób".

Istotne znaczenie dla oceny analizowanego przepisu art. 67b ust. 15 ustawy o KSC będącego podstawą do wydania decyzji o uznaniu za dostawcę wysokiego ryzyka ma też to, że treść rozstrzygnięcia organu w żaden formalny sposób nie została powiązana z treścią opinii, którą ma obowiązek pozyskać minister właściwy do sprawy informatyzacji od Kolegium do spraw Cyberbezpieczeństwa na podstawie art. 67b ust. 10 ustawy o KSC, a które to Kolegium funkcjonuje przy Radzie Ministrów, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa na podstawie przepisu art. 64 ustawy o KSC. Jakkolwiek z treści przepisu art. 67b ust. 12 pkt 7 ustawy o KSC wynika, że sporządzoną w toku postępowania administracyjnego o uznaniu dostawcy za DWR przez Kolegium opinię przekazuje się ministrowi właściwemu do spraw informatyzacji, to z treści przepisów art. 67b ust. 15 i 16 ustawy o KSC nie wynika, żeby opinia ta i zawarta w niej analiza była w jakikolwiek sposób wiążąca dla organu przy wydawaniu decyzji o uznaniu dostawcy za DWR i miała wpływ na treść rozstrzygnięcia oraz uzasadnienia wydawanej decyzji. W konsekwencji, na gruncie przepisu art. 67b ust. 15 ustawy o KSC uzasadniony jest pogląd, że wydana na podstawie art.

67b ust. 10 ustawy o KSC, nawet jeśli zawiera elementy wskazane w art. 67b ust. 11 i 12 ustawy o KSC, to nie ma charakteru przesądzającego o treści rozstrzygnięcia organu.

Widoczny brak spójności przepisów regulujących przesłanki wszczęcia postępowania administracyjnego (art. 67b ust. 1 ustawy o KSC), przepisów regulujących zakres opinii sporządzanej przez Kolegium do spraw Cyberbezpieczeństwa (art. 67b ust. 10 i 11 ustawy o KSC) z przepisem regulującym kryteria oceny przedsiębiorcy za dostawcę wysokiego ryzyka w treści samej decyzji (art. 67b ust. 15 ustawy o KSC) może być podstawą do postawienia zarzutu o braku dochowania przez ustawodawcę wymogu zachowania należytej staranności przy tworzeniu prawa według którego ma działać organ, władczo rozstrzygając o prawach i wolnościach dostawcy sprzętu lub oprogramowania ICT, tj. zarzutu naruszenia art. 2 Konstytucji. Rozbieżność przesłanek ustawowych wszczęcia postępowania i wydania decyzji oraz brak wzajemnego powiązania pomiędzy nimi sprawia, że całe postępowanie administracyjne toczone na podstawie przepisu art. 67b ustawy o KSC będzie miało charakter arbitralny i będzie uzależnione jedynie od dowolnego uznania organu wydającego decyzję na podstawie art. 67b ust. 15 ustawy o KSC, jakie okoliczności będą uznane za „zagrożenie dla podstawowego interesu bezpieczeństwa państwa", a jakie nie i czy weźmie pod uwagę treść analizy sporządzonej w trybie art. 67b ust. 10 ustawy o KSC. W tym miejscu należy podkreślić, że zasada zaufania do państwa i stanowionego przez niego prawa opiera się na zapewnieniu pewności co do treści prawa, a więc na takim zespole cech przysługujących prawu stanowionemu, które zapewniają jednostce (przedsiębiorcy) bezpieczeństwo prawne, umożliwiając jednostce kształtowanie swoich stosunków życiowych lub gospodarczych na podstawie pełnej znajomości przesłanek działania organów państwowych oraz konsekwencji prawnych, jakie jej działania mogą pociągnąć za sobą. Jednostka (przedsiębiorca – dostawca sprzętu lub oprogramowania ICT) powinna mieć możliwość określenia konsekwencji poszczególnych zachowań i zdarzeń na podstawie obowiązującego prawa, a także zasadnie oczekiwać, że prawodawca nie zmieni tego prawa w sposób arbitralny i nie będzie go dowolnie stosował (wyroki Trybunału Konstytucyjnego z dnia: 14 czerwca 2000 r., sygn. akt P 3/00; 19 marca 2007 r., sygn. akt K 47/05 i 5 października 2010 r., sygn. akt K 16/08).

Trzecim kryterium oceny konstytucyjności przepisów regulujących odjęcie własności jest ocena kwestia proporcjonalności zastosowanych środków ingerencji przez organy władzy publicznej, tak aby mogły być one uznane za zgodne z wymaganiami art. 21 ust. 2 Konstytucji. Dokonanie takiej oceny należy rozpocząć od wskazania skutków wydania decyzji o uznaniu

przedsiębiorcy za dostawcę wysokiego ryzyka na podstawie przepisu art. 67b ust. 15 ustawy o KSC. Zgodnie z przepisem art. 67c ust. 1, 2 i 4 ustawy o KSC:

„Art. 67c. 1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o których 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;
2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka niepóźniej niż w terminie 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej "Monitor Polski".
2. Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.
4. Podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.), nie mogą nabywać typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji, o której mowa w art. 67b ust. 15."

Skutkiem zatem wydania decyzji o uznaniu przedsiębiorcy za dostawcę wysokiego ryzyka na podstawie przepisu art. 67b ust. 15 ustawy o KSC jest: 1) eliminacja dostawcy z rynku polskiego dla podmiotów kluczowych oraz ważnych, 2) eliminacja z rynku produktów dostawcy, jeśli jego produkty już zostały wprowadzone na rynek oraz 3) brak możliwości oferowania przez dostawcę swoich produktów podmiotom, które zobowiązane są do stosowania zakupów w trybie i na zasadach opisanych w Prawie zamówień publicznych. Analizowana regulacja wywołuje od strony ekonomicznej skutki w majątku dostawcy objętego decyzją DWR, w majątkach podmiotów kluczowych i zależnych (zakaz użytkowania i nakaz wymiany sprzętu lub oprogramowania objętego decyzją) oraz w majątkach podmiotów zobowiązanych do stosowania zamówień publicznych. Wydawana na podstawie art. 67b ust. 15 ustawy o KSC decyzja rozszerza zatem skutek ekonomiczny odjęcia własności polegający na braku możliwości oferowania produktów i usług na rynku przez dostawcę (skutek jednostkowy) o nałożenie obowiązku wymiany już zakupionego i użytkowanego sprzętu lub oprogramowania przez podmioty zobowiązane do stosowania ustawy o KSC (skutek

wielopodmiotowy). W tym miejscu należy od razu dodać, że skutki ekonomiczne takiej decyzji o uznaniu DWR wydawanej przez ministra właściwego do spraw informatyzacji nie są w żaden sposób rekompensowane przez Skarb Państwa. Ustawa o KSC nie przewiduje żadnych mechanizmów finansowego wsparcia dla adresata decyzji o uznaniu za DWR w postaci odszkodowania oraz podmiotów dotkniętych skutkami takiej decyzji (zwrot kosztów przymusowej wymiany sprzętu lub oprogramowania ICT). Tylko z tej przyczyny braku mechanizmu finansowej rekompensaty należy uznać, że przepisy art. 67c ust. 1, 2 i 4 ustawy o KSC wprowadzają do tej ustawy rozwiązania prawne, które rażąco odbiegają od standardu przewidzianego dla przepisów odejmujących własność - art. 64 ust. 2 i 3 Konstytucji oraz art. 31 ust. 3 zd. 2 Konstytucji.

W ocenie wnioskodawcy, regulacja prawna, której istota sprowadza się do odjęcia przedsiębiorcy prawa do pobierania pożytków ze sprzedaży rzeczy ruchomej (sprzętu) lub praw na dobrach niematerialnych (oprogramowania) w drodze decyzji administracyjnej i to natychmiast wykonalnej stanowi nadmierną i daleko idącą ingerencję w prawo własności zdefiniowane w art. 64 ust. 1, 2 i 3 Konstytucji, który przewidują konstytucyjną gwarancję ochrony własności od strony podmiotowej (tzn. przez ujęcie ochrony konkretnego prawa lub rzeczy będącego w dyspozycji konkretnej osoby). W sytuacji, w której zastosowany akt władczy (decyzja administracyjna) dotyczy konkretnego i indywidualnego przedsiębiorcy, to skutek tego aktu nie dotyczy wyłącznie odebrania własności rzeczy jak to ma miejsce w przypadku wywłaszczenia z nieruchomości, ale odebrania przedsiębiorcy możliwości zarobkowania na rynku ze skutkiem natychmiastowym i na przyszłość (wywłaszczenie z rynku) poprzez faktyczny brak możliwości prowadzenia dalszej działalności gospodarczej. Dla oceny konstytucyjności tych przepisów znaczenie ma też to, że decyzja wydana na podstawie art. 67b ust. 15 ustawy o KSC jest natychmiast wykonalna (art. 67b ust. 18 ustawy o KSC) oraz że od decyzji wydanej przez organ nie przysługuje wniosek o ponowne rozpatrzenie sprawy (art. 67b ust. 19 ustawy o KSC). Ponadto ustawodawca nie wprowadził żadnego zróżnicowania stopnia dolegliwości wydawanej decyzji, np. w zależności od stopnia zawinienia dostawcy lub wielkości incydentu, który mógł lub też wywołał zagrożenie bezpieczeństwa państwa. Organ wydający decyzję nie może też samodzielnie ograniczyć (zmiarkować) dolegliwości wynikającej z wydanej decyzji lub wybrać rodzaj dolegliwości dla dostawcy, który mógłby mieć charakter bardziej adekwatny dla niego i wywołanego stopnia zagrożenia. W świetle tak skonstruowanych przepisów trudno jest mówić o zachowaniu proporcjonalności przyjętych rozwiązań prawnych, gdyż z samego faktu wydania decyzji o uznaniu przedsiębiorcy za

dostawcę wysokiego ryzyka skutki prawne są przez ustawodawcę wskazane wprost w art. 67c ust. 1, 2 i 4 ustawy o KSC i nie mogą podlegać ani modyfikacji, ani też stopniowaniu. W konsekwencji uprawniony jest pogląd, że przy takiej konstrukcji przepisów art. 67b ustawy o KSC samo wydanie decyzji może być traktowane jako rodzaj sankcji o skutku represyjnym dla przedsiębiorcy zbliżonym do sankcji karnej zaostrzonej o brak jakiejkolwiek ekwiwalentności ze strony Skarbu Państwa związanej z odjęciem własności.

Reasumując, na gruncie aksjologii konstytucyjnej ustawa zasadnicza zapewnia każdemu podmiotowi poszanowanie jego prawa do własności (art. 64 ust. 1), a także proklamuje równą dla wszystkich ochronę prawa własności (art. 64 ust. 2). Konstytucja zastrzega także, iż własność może być ograniczona tylko w drodze ustawy i tylko w zakresie, w jakim nie narusza ona istoty prawa własności (art. 64 ust. 3). Podkreślone to jest przez samą systematykę Konstytucji, która umieszcza art. 64 na samym początku podrozdziału odnoszącego się do wolności i praw ekonomicznych, socjalnych i kulturalnych. W doktrynie wskazuje się, iż *„nie jest to przypadkowe i nawiązuje do zasad ustrojowych i oparcia społecznej gospodarki rynkowej na własności prywatnej*" - B. Banaszak, Konstytucja Rzeczypospolitej Polskiej, Komentarz, Warszawa 2012, str. 385). W konstytucyjnym porządku prawnym fundamentalne znaczenie prawa własności wyraża wprost art. 21 ust. 1 Konstytucji, który ustanawia ochronę prawa własności jako jedną z podstawowych zasad ustroju Rzeczypospolitej Polskiej. Potwierdza to treść ust. 2 tego artykułu, który konstytucjonalizuje standardy jej odjęcia na cele publiczne. Własność prywatna w art. 20 Konstytucji określana jest także jako jeden z wyznaczników społecznej gospodarki rynkowej, będącej podstawą ustroju gospodarczego Rzeczypospolitej Polskiej. Korelatem tych zasad ustrojowych jest ochrona prawa własności jako podstawowego konstytucyjnego prawa podmiotowego o charakterze majątkowym gwarantowanego w różnych aspektach przez art. 64 Konstytucji.

Na tle art. 64 ust. 1 Konstytucji zapadło bardzo wiele orzeczeń Trybunału Konstytucyjnego i biorąc pod uwagę przeprowadzoną powyżej analizę trzeba przytoczyć choćby te szczególnie istotne z punktu widzenia konstytucyjnych dyrektyw (wskazówek) dla ustawodawcy, który reguluje kwestię własności *sensu largo*. Prawo własności jest *„najpełniejszym z praw majątkowych*" (zob. m.in. wyrok TK z 12 stycznia 2000 r. w sprawie P 11/98), *„Konstytucyjna ochrona własności oznacza przede wszystkim prawo do spokojnego korzystania z własności, co jest równoznaczne z nakazem nieingerencji we własność ze strony władz publicznych*" (wyrok TK z 14 października 2009 r. w sprawie Kp 4/09). W analizowanej

sprawie ingerencja ustawodawcy dotyczy *stricte* odjęcia możliwości zbycia „sprzętu lub oprogramowania" na rynku (wprowadzenia do obrotu) (art. 67b ust. 15 ustawy o KSC) podmiotowi, który na mocy decyzji ministra właściwego do spraw informatyzacji został uznany za dostawcę wysokiego ryzyka, a tym samym pozbawienie możliwości eksploatowania takiego „sprzętu lub oprogramowania" przez podmioty kluczowe oraz podmioty ważne, a także pobierania przez przedsiębiorcę będącego dostawcą takiego sprzętu lub oprogramowania z nich pożytków w ramach prowadzonej działalności gospodarczej, co wprost narusza nakaz braku ingerowania w prywatną własność wywodzony właśnie z art. 64 ust. 1 Konstytucji. Przepisy ustawowe nie mogą bowiem niweczyć podstawowych uprawnień składających się na treść prawa własności, takich jak możliwość korzystania, pobierania pożytków lub pośredniego eksploatowania przedmiotu własności i to bez zapewnionego odszkodowania z tytułu odjęcia własności.

Przepis art. 64 ust. 1 Konstytucji nakłada na ustawodawcę „*obowiązek kształtowania prawa własności i poszczególnych praw podmiotowych o charakterze ekonomicznym w taki sposób, aby zapewnić możliwość czynienia z nich użytku oraz zagwarantować im odpowiednią ochronę. Z przepisu tego wynikają obowiązki ustawodawcy: pozytywny, tj. ustanowienia procedur ochrony tych praw, oraz negatywny, tj. powstrzymywania się od regulacji, które owe prawa mogłyby pozbawiać ochrony prawnej lub ją ograniczać*" (wyrok TK z dnia 25 października 2016 r., sygn. SK 71/13). W orzecznictwie TK podkreśla się przy tym, iż art. 64 ust. 1 Konstytucji stanowi rozwinięcie i uszczegółowienie ogólnej zasady ochrony własności wyrażonej w art. 21 ust. 1 Konstytucji (por. wyrok TK z 13 kwietnia 1999 r., sygn. K 36/98). Prawo własności i jego gwarancje wskazane w art. 64 Konstytucji należy interpretować w świetle zasad ustroju Rzeczypospolitej, w szczególności art. 2 i art. 20 Konstytucji. Własność prywatna jest bowiem zaliczana do podstawowych zasad ustrojowych państwa. Oznacza to, że konstytucyjnej ochronie prawnej podlega istota własności jako prawa podmiotowego, tj. autonomia zarządzania swoim majątkiem przez podmioty prawa i samodzielne decydowanie o sposobach gospodarowania tym mieniem w oparciu o posiadaną autonomię na własny rachunek i na własne ryzyko. Przepis art. 20 należy łączyć z art. 2 Konstytucji, stanowiącym, iż Rzeczpospolita Polska jest demokratycznym państwem prawnym urzeczywistniającym zasady sprawiedliwości społecznej (wyrok Trybunału Konstytucyjnego z dnia 29 lipca 2013 r., sygn. SK 12/12). Korzystanie zatem z każdego prawa podmiotowego, w tym także prawa własności i prawa posiadania, podlega konstytucyjnej ochronie przed nadmierną ingerencją ustawodawcy, która mogłaby przekształcić je w pusty zapis, wydrążony z rzeczywistych treści (*ius nudum*).

Biorąc pod uwagę powyższe kryteria oceny konstytucyjności i wskazane powyżej wątpliwości co do treści art. 67b ustawy o KSC wprowadzony ustawą z dnia 23 stycznia 2026 r., uzasadnione są podniesione powyżej zarzuty co do jego zgodności z art. 64 ust. 1, 2 i 3 w związku z art. 31 ust. 3 Konstytucji oraz w związku z art. 2, art. 20 oraz 21 ust. 2 Konstytucji. Przepis art. 67b ustawy o KSC nie spełnia wymogu legalności oraz proporcjonalności i prowadzi do naruszenia nakazu równego traktowania przedsiębiorców poprzez zastosowanie środka prawnego w postaci wykluczenia towarów lub usług (sprzętu lub oprogramowania ICT) określonych podmiotów z rynku, bez poszukiwania jakichkolwiek innych możliwych rozwiązań, zgodnie z zasadą proporcjonalności oraz bez zapewnienia jakiejkolwiek rekompensaty z tytułu wydanej decyzji zarówno dla jej adresata, jak i dla podmiotów korzystających ze sprzętu lub oprogramowania ICT dostarczonego przez podmiot uznany za dostawcę wysokiego ryzyka.

Zarzut nr 2

Niezgodność art. 67e ust. 1 i 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) dodanego ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252) – z art. 45 ust. 1 w związku z art. 31 ust. 3 Konstytucji oraz z art. 78 w związku z art. 31 ust. 3 Konstytucji w zakresie jakim przepisy te ograniczają w sposób nieproporcjonalny prawo strony postępowania administracyjnego do jawnego postępowania sądowego ze skargi na decyzję organu właściwego ds. cyberbezpieczeństwa wydanej na podstawie przepisu art. 67b ust. 15 ustawy o krajowym systemie cyberbezpieczeństwa oraz w zakresie w jakim przepisy te przewidują doręczenie skarżącemu odpisu wyroku sądu administracyjnego bez tej części uzasadnienia, której utajnienie nie jest konieczne dla ochrony informacji niejawnych.

Zarzut nr 3

Niezgodność art. 67b ust. 2, 6, 8, 10-13 i 17-19 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) dodanego ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252) – z art. 2, art. 7, art. 51 ust. 3 oraz art. 78 w związku z art. 31 ust. 3 Konstytucji w zakresie jakim przepisy te nie zapewniają możliwości przeprowadzenia rzetelnego postępowania administracyjnego w toku

postępowania zmierzającego do wydania decyzji na podstawie przepisu art. 67b ust. 15 ustawy o KSC poprzez ograniczenie stronie tego postępowania możliwości zapoznania się ze zgromadzonym w sprawie materiałem dowodowym, w tym z opinią sporządzoną przez Kolegium ds. Cyberbezpieczeństwa na podstawie art. 67b ust. 10 ustawy o KSC, a tym samym ograniczenie możliwości wypowiedzenia się wobec zgromadzonego materiału dowodowego i sformułowanych na jego podstawie zarzutów będących podstawą do rozstrzygnięcia na podstawie przepisu art. 67b ust. 15 ustawy o KSC.

Analizowane przepisy Rozdziału 12a ustawy o KSC (art. 67a – art. 67f), które wprowadzają szczególny mechanizm nadzoru rynku sprzętu lub oprogramowania ICT w rozumieniu art. 2 pkt 11k, 111 k i 11m ustawy o KSC pozwalający organom nadzoru na uznanie określonego dostawcy sprzętu lub oprogramowania ICT dla podmiotów kluczowych i ważnych w rozumieniu Załącznika nr 1 i 2 do ustawy o KSC, za dostawcę wysokiego ryzyka (DWR) zawierają także przepisy szczególne regulujące zasady kontroli sądowej decyzji o uznaniu za dostawcę wysokiego ryzyka (art. 67e ust. 1 i 2 ustawy o KSC). Treść tych przepisów dotyczy dwóch elementów postępowania sądowo-administracyjnego, tj.:

a) wskazania, że sąd administracyjny rozpatrujący skargę na decyzję organu o uznaniu za dostawcę wysokiego ryzyka wydaną na podstawie art. 67b ust. 15 ustawy o KSC orzeka na posiedzeniu niejawnym w składzie trzech sędziów;

b) ograniczenia jawności treści wyroku i uzasadnienia dla strony, która może otrzymać jedynie wyrok wraz z uzasadnieniem w tej części, która nie zawiera informacji niejawnych.

W ocenie wnioskodawcy, powyżej wskazana regulacja zawarta w art. 67e ustawy o KSC ingeruje w sposób nieproporcjonalny w konstytucyjne prawo do sądu w zakresie w jakim ustawodawca ogranicza jawność rozprawy (art. 45 ust. 2 Konstytucji w zw. z art. 90 § 1 Prawa o postępowaniu przed sądami administracyjnymi – dalej jako „P.p.s.a.") w postępowaniu sądowym ze skargi na decyzję wydaną na podstawie art. 67b ust. 15 ustawy o KSC oraz prawo do zapoznania się z treścią uzasadnienia do wydanego przez sąd orzeczenia (art. 45 ust. 1 i 2 Konstytucji w zw. z art. 142 § 1 i 2 P.p.s.a.) przez stronę w tym postępowaniu. Stąd też przepisy te powinny zostać przeanalizowane w kontekście wymogu występowania interesu publicznego w postaci bezpieczeństwa państwa oraz porządku publicznego we wprowadzeniu tych ograniczeń, a co wynika wprost z normy zawartej w art. 45 ust. 1 oraz art. 78 Konstytucji.

Na gruncie art. 45 ust. 2 Konstytucji wynikająca z art. 45 ust. 1 Konstytucji zasada jawności rozprawy może podlegać ograniczeniom wskazanym w tym przepisie, tj. z uwagi na: moralność, bezpieczeństwo państwa i porządek publiczny, ochronę życia prywatnego stron lub inny ważny interes prywatny. Jednak ewentualne ograniczenia od zasady jawnego rozpatrywania spraw przez sąd powinny mieć charakter proporcjonalny w rozumieniu art. 31 ust. 3 Konstytucji i które nie powinny w sposób nadmierny wpływać na rzetelność całego postępowania sądowego oraz dawać możliwości podejmowania arbitralnych decyzji przez skład orzekający. Biorąc pod uwagę specyfikę postępowania sądowo-administracyjnego, które jest narzędziem sądowej kontroli decyzji administracyjnych lub innych aktów wydawanych przez organy administracji państwowej, szczególne znaczenie dla zapewnienia możliwości obrony własnych interesów przez stronę postępowania administracyjnego ma:

1) możliwość do zapoznania się z całością materiału dowodowego zgromadzonego przez organ w toku postępowania;
2) możliwość zgłaszania wniosków dowodowych i aktywnego udziału w postępowaniu dowodowym;
3) możliwość weryfikacji wydawanych w pierwszej instancji rozstrzygnięć merytorycznych i proceduralnych przez organ wyższej instancji;
4) konieczność rzetelnego i wiarygodnego uzasadnienia wydawanych decyzji, które mogą być podstawą do zastosowania środków odwoławczych przewidzianych prawem;
5) konieczność stosowania przez organ przepisów proceduralnych w sposób i terminie umożliwiającym stronie zajęcie stanowiska w toku postępowania;
6) brak arbitralnego stosowania prawa przez organ;
7) ignorowanie obowiązującego prawa i odmowa jego stosowania przez organ.

Natomiast w postępowaniu sądowo-administracyjnym jedną z kluczowych gwarancji rzetelnego postępowania sądowego rozumianych jako sprawiedliwość proceduralna jest zapewnienie stronie możliwości udziału w czynnościach sądowych i przedstawienia swojego stanowiska sądowi czy to osobiście, czy z pomocą pełnomocnika procesowego. Zasada jawności postępowania w swojej zasadniczej warstwie dotyczy bowiem gwarancji dostępu do sądu dla strony postępowania, tj. zapewnienia możliwości bycia wysłuchanym przez sąd, który jako organ niezawisły i niezależny jest obowiązany do rzetelnej oceny sytuacji prawnej skarżącego.

W dorobku orzeczniczym Trybunału Konstytucyjnego podkreśla się, że: *„(...) Pojęcie sprawiedliwości proceduralnej nie ma ściśle sprecyzowanego znaczenia. Różne koncepcje sprawiedliwości proceduralnej mają jednak wspólne jądro, sprowadzające się do:*
- możności bycia wysłuchanym,
- ujawniania w czytelny sposób motywów rozstrzygnięcia, w stopniu umożliwiającym weryfikację sposobu myślenia sądu (i to nawet jeśli samo rozstrzygnięcie jest niezaskarżalne - legitymizacja przez przejrzystość), a więc unikania dowolności czy wręcz arbitralności w działaniu sądu,
- zapewnienia przewidywalności dla uczestnika postępowania, przez odpowiednią spójność i wewnętrzną logikę mechanizmów, którym jest poddany.
Tak określone cechy istotne sprawiedliwości proceduralnej znajdują potwierdzenie w analizie konstytucyjnego statusu władzy sądowniczej. Sąd nawet jeśli rozpatruje sprawę w postępowaniu kasacyjnymi, musi zachować swoją tożsamość konstytucyjną wyznaczoną przez zastane pojęcie władzy sądowniczej. Tożsamość konstytucyjna sądu (wymiaru sprawiedliwości) jest wyznaczana - poza oczywistym wymogiem niezależności, bezstronności i niezawisłości - między innymi przez:
- odrzucenie dowolności i arbitralności,
- zapewnienie udziału zainteresowanych podmiotów w postępowaniu,
- traktowaniu jawności jako zasady,
- wydawaniu rozstrzygnięć zawierających rzetelne, weryfikowalne uzasadnienia." - por. wyrok TK z dnia 16 stycznia 2006 r., sygn. SK 30/05.

Wskazany powyżej wzorzec kontroli konstytucyjnej umożliwia odniesienie się do regulacji przepisu art. 67e ust. 1 ustawy o KSC nakazującej sądowi administracyjnemu rozpatrywanie spraw ze skargi na decyzję wydaną na podstawie art. 67b ust. 15 ustawy o KSC na posiedzeniu niejawnym oraz przepisu art. 67e ust. 2 ustawy o KSC ograniczającego dostęp do treści uzasadnienia wyroku skarżącemu w części w jakiej zawiera ono informacje niejawne w rozumieniu przepisów o ochronie informacji niejawnych. Punktem wyjścia do dalszej analizy powinno być wskazanie, że zgodnie z obowiązującą regulacją art. 90 § 1 P.p.s.a., jako zasada ustawowa funkcjonuje jawność posiedzeń sądowych, która z mocy przepisów szczególnych może jednak zostać wyłączona. Taki wyjątek znajduje się w art. 38 ust. 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209) wskazujący, że: „Sąd administracyjny rozpatruje skargę na posiedzeniu niejawnym". Praktycznym skutkiem takiego wyłączenia jest brak obowiązku rozpatrzenia skargi na rozprawie z udziałem stron oraz

publiczności. Dodatkowym skutkiem takiej regulacji jest też brak możliwości zastosowania przez skład orzekający art. 90 § 2 P.p.s.a. pozwalającego skierowanie sprawy na posiedzenie jawne także wtedy, gdy sprawa podlega rozpoznaniu na posiedzeniu niejawnym. Innymi słowy, zasadniczym skutkiem wyłączenia jawnego rozpoznawania sprawy przez ustawodawcę jest wyłączenie możliwości wysłuchania strony postępowania przez sąd i przedstawienia w sposób ustny oraz bezpośredni wobec składu orzekającego oraz organu argumentów przez stronę lub jej pełnomocnika i ich uzasadnienia. Prowadzone postępowanie sądowe ma wówczas charakter wyłącznie pisemny.

W ocenie wnioskodawcy możliwość rozpoznania sprawy przez sąd administracyjny na posiedzeniu niejawnym sama w sobie nie ma charakteru ograniczającego prawo do sprawiedliwego (rzetelnego) postępowania sądowego w rozumieniu art. 45 ust. 1 Konstytucji. Może być jednym z elementów postępowania, który wpływa na szybkość rozpatrzenia skargi i co w sprawach administracyjnych o charakterze mało skomplikowanym, gdzie materiał dowodowy jest ograniczony a organ działa na wniosek strony, to wówczas jest to mechanizm prawny ułatwiający sprawowanie wymiaru sprawiedliwości. Elementem różnicującym i wpływającym na negatywną ocenę przepisu art. 67e ust. 1 ustawy o KSC jest sam charakter postępowania administracyjnego prowadzonego na podstawie art. 67b ustawy o KSC, które nie toczy się z inicjatywy strony postępowania a z urzędu, tj. z inicjatywy organu nadzoru rynku – por. art. 67b ust. 1 ustawy o KSC i które ma charakter śledczy względem strony poddanej procedurze uznania za dostawcę wysokiego ryzyka (DWR). Celem takiego postępowania nie jest bowiem przyznanie stronie jakiegoś uprawnienia, np. wydanie pozwolenia na budowę czy nadanie określonych uprawnień w postaci prawa jazdy, a weryfikacja hipotezy o szkodliwości sprzętu lub oprogramowania ICT, a w konsekwencji wydania decyzji eliminacja konkretnego podmiotu z rynku dostaw sprzętu lub oprogramowania ICT w rozumieniu ustawy o KSC. W tym kontekście wyłączenie jawności rozprawy sądowej badającej legalność decyzji administracyjnej wydanej na podstawie art. 67b ust. 15 ustawy o KSC jest tylko jednym z elementów całego postępowania prowadzonego przez organ ds. cyberbezpieczeństwa, które toczy się w logice postępowania śledczego. Na taką ocenę tego szczególnego typu postępowania administracyjnego składają się następujące elementy ograniczające gwarancje rzetelności po stronie organu i wpływające na możliwość obrony swoich interesów przez stronę postępowania takie jak:

1) jednoinstancyjność postępowania administracyjnego (art. 67b ust. 19 ustawy o KSC);

2) natychmiastowa wykonalność decyzji wydanej na podstawie art. 67 ust. 15 ustawy o KSC (art. 67b ust. 18 ustawy o KSC);
3) wyłączenie przepisów art. 28, art. 31, art. 51, art. 66a i art. 79 Kodeksu postępowania administracyjnego (art. 67b ust. 2 ustawy o KSC);
4) upublicznienie informacji o fakcie wszczęcia postępowania w przedmiocie uznania za dostawcę wysokiego ryzyka i brak gwarancji anonimowości strony takiego postępowania (art. 67b ust. 6 i 8 ustawy o KSC);
5) upublicznienie informacji o fakcie wydania decyzji o uznaniu za dostawcę wysokiego ryzyka (art. 67b ust. 17 ustawy o KSC);
6) brak możliwości dostępu przez stronę do treści opinii wydanej przez Kolegium ds. Cyberbezpieczeństwa sporządzonej zgodnie z art. 67b ust. 11 – 13 ustawy o KSC.

W konsekwencji tak ukształtowanego postępowania administracyjnego w przedmiocie uznania za dostawcę wysokiego ryzyka, prawo do obrony przez stronę jej własnych interesów, czyli możliwości sprzedaży (wprowadzania do obrotu) sprzętu lub oprogramowania ICT zostało przez ustawodawcę znacznie ograniczone, a całe postępowanie nabiera cech typowego postępowania inkwizycyjnego, gdzie strona jest w praktyce przedmiotem postępowania, a nie pełnoprawnym jego uczestnikiem z gwarancjami obrony własnych interesów w toku postępowania tak administracyjnego, jak i sądowo-administracyjnego. W ocenie wnioskodawcy, brak dostępu do zasadniczego elementu materiału dowodowego zgromadzonego przez organ jaką jest opinia sporządzona przez Kolegium uniemożliwia stronie skuteczne zaskarżenie rozstrzygnięcia zarówno w toku postępowania administracyjnego, jak i sądowo administracyjnego, co skutkuje naruszeniem art. 51 ust. 3 oraz art. 78 w związku z art. 31 ust. 3 Konstytucji. Zaskarżone przepisy ustawy o KSC wprost ograniczają dostęp do akt postępowania administracyjnego i przewidują sankcjonowanie strony polegające na upublicznieniu informacji o samym fakcie rozpoczęcia postępowania w przedmiocie uznania za dostawcę wysokiego ryzyka (brak anonimowości strony i brak stosowania zasady domniemania niewinności). Biorąc pod uwagę to, że z art. 51 ust. 3 i 4 Konstytucji wynikają standardy sprawiedliwego (rzetelnego) postępowania administracyjnego, stanowiące jeden z istotnych elementów zasady państwa prawnego, dlatego też ustawowe ograniczenia prawa dostępu strony do dotyczących jej urzędowych dokumentów i zbiorów danych w rozumieniu art. 51 ust. 3 Konstytucji należy rozpatrywać łącznie z art. 31 ust. 3 Konstytucji, a więc przez pryzmat testu proporcjonalności w stosowaniu przez ustawodawcę ograniczeń praw i wolności obywatelskich. W analogiczny sposób argumentował już Trybunał Konstytucyjny w wyroku z

dnia 20 października 2010 r., sygn. P 37/09, wskazując, że: „*Oceniając przestrzeganie przez ustawodawcę konstytucyjnych standardów sprawiedliwości proceduralnej, należy uwzględnić zawsze przedmiot i specyfikę danego postępowania. (...) Gwarancje konstytucyjne związane z prawem do sądu nie mogą być w konsekwencji traktowane jako nakaz urzeczywistnienia w każdym trybie i w każdym rodzaju procedury tego samego zestawu instrumentów procesowych, jednolicie określających pozycję stron postępowania i zakres przysługujących im środków procesowych.*". Z uwagi na specyficzny cel postępowania administracyjnego w przedmiocie uznania za dostawcę wysokiego ryzyka ocena całości wskazanych w treści zarzutu ograniczeń w dostępie do rzetelnego postępowania administracyjnego wskazanych w pkt 6 a mogącego skutkować wydaniem decyzji zakazującej sprzedaży sprzętu lub oprogramowania ICT przez konkretnego dostawcę nosi znamiona nieproporcjonalnego ograniczenia praw i wolności strony postępowania.

Dopiero w tym kontekście widać, że wyłączenie przez ustawodawcę możliwości przeprowadzenia jawnej rozprawy przed sądem (art. 67e ust. 1 ustawy o KSC) oraz pozbawienie możliwości zapoznania się z uzasadnieniem wyroku w części objętej ochroną informacji niejawnych są tylko elementami dopełniającymi ograniczenie prawa do obrony swoich interesów przez stronę już w samym postępowaniu administracyjnym o uznaniu za DWR. Z tego też względu oba zarzuty uzasadniane są wspólnie. Jakkolwiek na gruncie art. 45 ust. 2 Konstytucji dopuszczalne jest ograniczenie jawności rozprawy m.in. z uwagi na bezpieczeństwo państwa i porządek publiczny, a co ustawodawca sfomułował w art. 67b ust. 15 ustawy o KSC w postaci przesłanki „zagrożenia dla podstawowego interesu bezpieczeństwa państwa", to w kontekście całości przyjętych przez ustawodawcę rozwiązań zawartych w art. 67b i art. 67e ustawy o KSC uprawniony jest wniosek, że strona postępowania w wyniku zastosowanych ograniczeń w jawności rozprawy, w dostępie do materiału dowodowego oraz do treści uzasadnienia wyroku może w ogóle nie dowiedzieć się ani też zweryfikować, z jakich względów została podjęta decyzja o uznaniu za dostawcę wysokiego ryzyka. W ocenie Wnioskodawcy, brak doręczenia stronie uzasadnienia wyroku sądu administracyjnego bądź jak literalnie wskazuje ustawodawca doręczenie wyroku, ale bez elementów uzasadnienia objętych ochroną informacji niejawnych, wprost prowadzi do ograniczenia jednego ze standardów proceduralnych, które należy wiązać z art. 45 ust. 1 i art. 78 Konstytucji, tj. ujawnienia w czytelny sposób motywów rozstrzygnięcia, w stopniu umożliwiającym weryfikację sposobu myślenia sądu, w celu uniknięcia dowolności czy wręcz arbitralności wydanego orzeczenia. Poznanie uzasadnienia rozstrzygnięcia jest kluczowe dla możliwości skutecznego zaskarżenia

orzeczenia sądu. Uzasadnienie wymusza bowiem samokontrolę sądu, który musi wykazać, że orzeczenie jest materialnie i formalnie prawidłowe, dokumentuje argumenty przemawiające za przyjętym rozstrzygnięciem, jest podstawą kontroli zewnętrznej przez organy wyższej instancji oraz służy indywidualnej akceptacji orzeczenia. Strona pozbawiona uzasadnienia w całości lub w części nie może zweryfikować toku myślenia sądu, co w konsekwencji ogranicza prawo do skutecznego zaskarżenia wyroku do Naczelnego Sądu Administracyjnego przy użyciu skargi kasacyjnej. Prawo do sądu nie może być rozumiane jedynie formalnie jako teoretyczna dostępność drogi sądowej zapisana w prawie, ale także materialnie, jako realna możliwość skutecznej ochrony na drodze sądowej, chociażby w drodze i tak mocno sformalizowanej czynności, jaką jest skarga kasacyjna w postępowaniu sądowo-administracyjnym. Biorąc pod uwagę obowiązujący przed sądem kasacyjnym przymus adwokacko-radcowski brak dostępu do materiału dowodowego oraz do uzasadnienia wyroku w części merytorycznej może w praktyce uniemożliwić pełnomocnikowi poprawne sformułowanie zarzutów kasacyjnych względem wyroku sądu I instancji.

Analiza całości przepisu art. 67b ustawy o KSC wskazuje, że kluczowym elementem całego materiału dowodowego w przedmiocie uznania za dostawcę wysokiego ryzyka jest opinia Kolegium ds. Cyberbezpieczeństwa sporządzana na podstawie art. 67b ust. 10 – 12 ustawy o KSC. Zgodnie z przepisem art. 67b ust. 13 pkt 7 ustawy o KSC ustalona przez Kolegium opinia przekazywana jest ministrowi właściwemu ds. informatyzacji celem wydania na jej podstawie decyzji – argument z art. 67b ust. 10 ustawy o KSC. Ustawa nie rozstrzyga natomiast jednoznacznie tego czy opinia Kolegium jest dostępna dla strony postępowania w przedmiocie uznania za dostawcę wysokiego ryzyka, a co ma istotne znaczenie w kontekście wiarygodności postępowania dowodowego i możliwości wypowiedzenia się przez stronę odnośnie zgromadzonego materiału dowodowego (art. 81 K.p.a.), a także w kontekście możliwości złożenia skargi do sądu administracyjnego na już wydaną decyzję na podstawie art. 67b ust. 15 ustawy o KSC. Złożenie skargi wyłącznie na podstawie treści wydanej decyzji administracyjnej, bez możliwości dostępu do kluczowego materiału dowodowego (opinii Kolegium) czyni możliwość realizacji prawa do sądu iluzorycznym (*ius nudum*). Biorąc pod uwagę to, że przesłanką do wydania decyzji o uznaniu za dostawcę wysokiego ryzyka jest okoliczność „zagrożenia dla podstawowego interesu bezpieczeństwa państwa", to racjonalnym i uzasadnionym będzie założenie, że zarówno zgromadzony materiał dowodowy oraz opinia Kolegium ds. Cyberbezpieczeństwa wydana na podstawie art. 67b ust. 10 ustawy o KSC będą miały charakter niejawny w rozumieniu ustawy o ochronie informacji niejawnych. Ten sposób rozumowania potwierdza przepis art. 67e ust. 2 zd. drugie ustawy o KSC wskazujący, że

Skarżący może otrzymać uzasadnienie do wyroku „z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych". Taka treść przepisu wskazuje, że także treść uzasadnienia decyzji wydana na podstawie art. 67b ust. 15 ustawy o KSC będzie miała charakter niejawny, choć nie wynika to wprost z treści tego przepisu.

W tak skonstruowanym postępowaniu administracyjnym oraz sądowo-administracyjnym w przedmiocie uznania za dostawcę wysokiego ryzyka ustawodawca nie wskazał jednoznacznie czy strona, mając dostęp do informacji niejawnych na określonym poziomie (zastrzeżone, poufne, tajne, ściśle tajne lub inne) ma zagwarantowany dostęp do całości materiału dowodowego zgromadzonego przez organ, bądź osobiście bądź przez pełnomocnika dysponującego takimi uprawnieniami i będzie mogła zapoznać się również z uzasadnieniem do wyroku sądu administracyjnego w części niejawnej. Literalna wykładnia art. 67e ust. 2 zd. drugie ustawy o KSC prowadzi do wniosku, że bez względu na to czy strona ma poświadczenie bezpieczeństwa na poziomie gwarantującym dostęp do informacji niejawnych na odpowiednim poziomie, to i tak z mocy prawa nie będzie mogła zapoznać się z tą częścią uzasadnienia, która zawiera informacje niejawne. W konsekwencji dostęp strony do takiego uzasadnienia jest niemożliwy co w ocenie Wnioskodawcy świadczy o nieproporcjonalnym naruszeniu art. 45 ust. 1 w związku z art. 31 ust. 3 Konstytucji, gdyż możliwość zapoznania się z uzasadnieniem orzeczenia sądowego jest konstytutywnym elementem prawa do rzetelnego procesu sądowego. Na ten właśnie element wskazywał Trybunał Konstytucyjny w przywoływanym już wyroku z dnia 16 stycznia 2006 r., sygn. SK 30/05: *„(...) Podstawowe funkcje (istota) konstytucyjnego prawa do sprawiedliwego rozpatrzenia sprawy ściśle wiążą się z funkcjami, które powszechnie przypisuje się uzasadnieniom sądowym. (...) Uzasadnianie orzeczeń sądowych jest decydującym komponentem prawa do rzetelnego sądu. Uzasadnienie sądowe pełni następujące funkcje:*

- wymusza samokontrolę sądu, który musi wykazać, że orzeczenie jest materialnie i formalnie prawidłowe oraz odpowiada wymogom sprawiedliwości;

- dokumentuje argumenty przemawiające za przyjętym rozwiązaniem;

- jest podstawą kontroli zewnętrznej przez organy wyższych instancji;

- służy indywidualnej akceptacji orzeczenia;

- umacnia poczucie zaufania społecznego i demokratycznej kontroli nad wymiarem sprawiedliwości;

- wzmacnia bezpieczeństwo prawne.".

Kwestia możliwości utajnienia części uzasadnienia wyroku sądu administracyjnego była już analizowana przez Trybunał Konstytucyjny, który na tle przywoływanej już wcześniej regulacji art. 38 ust. 2 ustawy o ochronie informacji niejawnych w wyroku z dnia 23 marca 2018 r., sygn. SK 8/14, orzekł, że: *„(...) 8.3. Całkowite pozbawienie strony możliwości zapoznania się z uzasadnieniem wyroku sądu administracyjnego pierwszej instancji prowadzi do ograniczenia zasady sprawiedliwej (rzetelnej) procedury sądowej (art. 45 ust. 1 Konstytucji), a także prawa do zaskarżania orzeczeń wydanych w pierwszej instancji (art. 78 Konstytucji). Kwestionowany art. 38 ust. 3 ustawy o ochronie informacji, który przewiduje, że skarżącemu doręcza się jedynie odpis wyroku sądu administracyjnego bez jego uzasadnienia, uniemożliwia poznanie motywów rozstrzygnięcia zarówno prawnych, jak i faktycznych. Co więcej, do braku doręczenia uzasadnienia wyroku sądu administracyjnego dochodzi w sytuacji, w której samo postępowanie sądowe toczyło się z wyłączeniem jawności wewnętrznej, a co za tym idzie udziału skarżącego (zob. art. 38 ust. 2 ustawy o ochronie informacji).”.*

Biorąc pod uwagę powyższe kryteria oceny konstytucyjności i wskazane powyżej wątpliwości co do treści art. 67e ust. 1 i 2 ustawy o KSC wprowadzonego ustawą z dnia 23 stycznia 2026 r., uzasadnione są podniesione powyżej zarzuty co do jego zgodności z art. 45 ust. 1 w związku z art. 31 ust. 3 Konstytucji oraz art. 78 w związku z art. 31 ust. 3 Konstytucji. Przepis art. 67e ust. 1 i 2 ustawy o KSC nie spełnia wymogu legalności oraz proporcjonalności we wprowadzaniu ograniczeń w jawności rozprawy sądowej oraz w dostępie do treści uzasadnienia wydanego orzeczenia. Przepisy art. 67e ust. 1 i 2 ustawy o KSC stosowane razem z przepisami art. 67b ust. 2, 6, 8, 10-13 i 17-19 ustawy o KSC, regulujące w sposób szczególny postępowanie administracyjne wobec podmiotu, który może zostać uznany za dostawcę wysokiego ryzyka, prowadzą do ograniczenia zasady sprawiedliwej (rzetelnej) procedury sądowej oraz sprawiedliwej (rzetelnej) procedury administracyjnej, a co godzi wprost w zasadę państwa prawnego (art. 2) oraz zasadę legalizmu działania organów administracji (art. 7).

Zarzut nr 4

Niezgodność art. 67g ust. 1, ust. 2, ust. 9 pkt 2, ust. 10 i ust. 11 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) dodanego ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252) - z art. 87 ust. 1 oraz z art. 149 ust. 1 w związku z art. 2 i art. 31 ust. 3 oraz z art. 64 ust. 2 Konstytucji w zakresie w jakim

wskazane powyżej przepisy upoważniają ministra właściwego do spraw administracji do nakładania obowiązku realizacji określonych zachowań (nakazów lub zakazów) podmiotom spoza administracji rządowej w drodze polecenia zabezpieczającego noszącego znamiona aktu prawa powszechnie obowiązującego w zakresie wskazanym w art. 67g ust. 10 ustawy o KSC oraz bez zapewnienia przez ustawodawcę jakiejkolwiek rekompensaty finansowej pokrywającej rzeczywiste koszty realizacji nałożonych takim aktem obowiązków.

Zarzut nr 5

Niezgodność art. 67g ust. 1, ust. 3 i 4, ust. 14 – 17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20) dodanego ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252) - z art. 2, art. 7 oraz art. 78 w związku z art. 31 ust. 3 Konstytucji w zakresie jakim przepisy te nie zapewniają możliwości przeprowadzenia sprawiedliwego (rzetelnego) postępowania administracyjnego w toku postępowania zmierzającego do wydania decyzji na podstawie przepisu art. 67g ust. 1 ustawy o KSC poprzez ograniczenie stronom tego postępowania możliwości udziału w nim, możliwości wypowiedzenia się wobec zgromadzonego materiału dowodowego, możliwości skorzystania z odwołania się od wydanego rozstrzygnięcia, natychmiastową wykonalność wydanego polecenia oraz poprzez brak indywidualnego zawiadomienia o wszczęciu postępowania i wydanym rozstrzygnięciu.

Analizowane przepisy Rozdziału 12a ustawy o KSC, niezależnie od przepisów wprowadzających szczególny mechanizm nadzoru rynku sprzętu lub oprogramowania ICT w rozumieniu art. 2 pkt 11k, 11l i 11m ustawy o KSC, regulują także zasady wydawania szczególnego typu aktu władczego, tj. polecenia zabezpieczającego wydawanego przez ministra właściwego do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego – art. 67g, art. 67h i art. 67i w związku z art. 2 pkt 6 ustawy o KSC. Zasadnicza treść tych przepisów reguluje szczególnego typu postępowanie administracyjne w ramach którego organ (minister właściwy do sprawy informatyzacji) może wydać w drodze decyzji administracyjnej, tzw. „polecenie zabezpieczające", którego treścią jest wskazanie określonego sposobu zachowania się przez podmiot kluczowy lub podmiot ważny zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się (art. 67g ust. 1, ust. 2, ust. 9 pkt 2 oraz ust. 10 i 11 ustawy o KSC).

Zgodnie z treścią art. 67g ust. 10 ustawy o KSC w ramach polecenia zabezpieczającego możliwe jest nakazanie przez właściwy organ określonego zachowania, o którym mowa w ust. 9 pkt 2 ustawy, polegającego na realizacji obowiązku:

1) przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;

2) realizacji przeglądu planów ciągłości działania, planów awaryjnych i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;

3) zastosowania określonej poprawki bezpieczeństwa w produkcie ICT lub usłudze ICT posiadającym daną podatność;

4) szczególnej konfiguracji produktu ICT lub usługi ICT, zabezpieczającej przed wykorzystaniem określonej podatności;

5) wzmożonego monitorowania zachowania systemu informacyjnego;

6) ograniczenia korzystania z określonego produktu ICT lub usługi ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego;

7) wprowadzenia ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego;

8) wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania;

9) zabezpieczenia określonych informacji, w tym dzienników systemowych;

10) wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.

Istotnym elementem konstrukcji prawnej polecenia zabezpieczającego jest jego generalny (zbiorowy) charakter wynikający wprost z art. 67g ust. 2 ustawy o KSC - „*Polecenie zabezpieczające dotyczy nieokreślonej liczby podmiotów kluczowych lub podmiotów ważnych oraz podmiotów finansowych, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554.*". W przepisie tym ustawodawca przesądził, że nie ma ono cech indywidualnego i konkretnego aktu organu o charakterze władczym rozstrzygającego sprawę administracyjną, ale ma ono charakter powszechny nakierowany wobec wszystkich podmiotów kluczowych i podmiotów ważnych w rozumieniu Załącznika nr 1 i nr 2 do ustawy o KSC, a więc w stosunku

do podmiotów funkcjonujących zarówno w ramach administracji państwowej (rządowej i samorządowej), jak i poza nią w prywatnym sektorze gospodarczym. Liczba podmiotów zobowiązanych do stosowania ustawy szacowana na etapie legislacyjnym wynosiła ok. 40.000. Wskazane w *art. 16 rozporządzenia UE (2022/2554) z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego* wyłączenie dotyczy jedynie części instytucji finansowych tam wskazanych. Tym samym, jakkolwiek polecenie zabezpieczające zostało ujęte przez ustawodawcę w formę decyzji administracyjnej (art. 67g ust. 1 ustawy o KSC), to jednak nie nosi ono cech specyficznych tego rodzaju aktu władczego organu wobec jego powszechnego charakteru i wobec braku możliwości odmowy jego wykonania. Skierowane jest ono bowiem nie wobec oznaczonej indywidualnie grupy podmiotów a wobec podmiotów wskazanych rodzajowo (podmioty kluczowe i podmioty ważne w rozumieniu Załącznika nr 1 i 2 do ustawy o KSC) do natychmiastowej realizacji bez gwarancji zachowania dwuinstancyjności postępowania administracyjnego i bez gwarancji rekompensaty przez organ kosztów wykonania tego polecenia. Za takim właśnie generalnym (zbiorowym) charakterem polecenia zabezpieczającego przemawiają również regulacje wskazujące, że:

1) zawiadomienie strony postępowania o czynnościach organu odbywa się poprzez publiczne opublikowanie informacji na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji – art. 67g ust. 4 ustawy o KSC;

2) ogłoszenie komunikatu o wydaniu polecenia zabezpieczającego obywa się w dzienniku urzędowym oraz na stronie internetowej urzędu obsługującego ministra właściwego do spraw informatyzacji – art. 67g ust. 15 ustawy o KSC;

3) polecenie zabezpieczające uznaje się za doręczone stronie z chwilą ogłoszenia komunikatu o wydaniu polecenia zabezpieczającego w dzienniku urzędowym ministra właściwego do spraw informatyzacji – art. 67g ust. 16 ustawy o KSC;

4) polecenie zabezpieczające ma charakter natychmiast wykonalny oraz nie przysługuje od niego żaden środek odwoławczy w procedurze administracyjnej – art. 67g ust. 14 i 17 ustawy o KSC;

5) brak wdrożenia polecenia zabezpieczającego lub odstąpienie od realizacji nakazów lub zakazów zawartych w poleceniu zabezpieczającym podlega karze administracyjnej – art. 73 ust. 1 pkt 20 i 21 ustawy o KSC;

6) do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się przepisów art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I ustawy z dnia 14 czerwca 1960 r. - Kodeks

postępowania administracyjnego, a pozostałe przepisy tej ustawy stosuje się jedynie odpowiednio – art. 67g ust. 3 ustawy o KSC.

W świetle tak ukształtowanej przez ustawodawcę konstrukcji prawnej polecenia zabezpieczającego należy postrzegać ten akt władczy organu bardziej jako rodzaj aktu powszechnie obowiązującego (normatywnego) niż klasycznie rozumianej decyzji administracyjnej wydawanej w indywidualnej sprawie. Taki charakter tego aktu będzie tym bardziej widoczny w sytuacji, w której organ wyda polecenie zabezpieczające mimo, iż część podmiotów kluczowych lub podmiotów ważnych nie będzie użytkowała sprzętu lub oprogramowania ICT objętego wydanym poleceniem. W związku z tym powstaje zasadnicze pytanie o dopuszczalność na gruncie art. 87 ust. 1 Konstytucji RP, przewidującej zamknięty katalog źródeł prawa powszechnie obowiązującego, tak skonstruowanego aktu władzy publicznej, jakim jest przewidziana w ustawie o KSC konstrukcja polecenia zabezpieczającego. Punktem wyjścia dla poniższej analizy powinien być przepis art. 149 ust. 1 Konstytucji wskazujący, że: „*Ministrowie kierują określonymi działami administracji rządowej lub wypełniają zadania wyznaczone im przez Prezesa Rady Ministrów. Zakres działania ministra kierującego działem administracji rządowej określają ustawy*". Przepis ten powinien być analizowany także razem z normą zawartą w art. 146 ust. 3 Konstytucji wskazującą, że: „*Rada Ministrów kieruje administracją rządową*", co wyznacza zakres uprawnień zarówno rządu jako organu konstytucyjnego, ale też i poszczególnych ministrów kierujących działami administracji rządowej. Nie budzi wątpliwości, że minister odpowiedzialny za poszczególne sprawy, które obejmuje konkretny dział administracji rządowej może formułować wobec podległych mu hierarchicznie osób i jednostek organizacyjnych nakazy określonego zachowania się. *A contrario* uprawnienie to nie przysługuje mu wobec osób i jednostek organizacyjnych, które nie są mu hierarchicznie podległe spoza administracji rządowej. Minister może też, na podstawie przepisów prawa materialnego wydawać decyzje administracyjne kształtujące w sposób indywidualny i konkretny sytuację prawną stron postępowania.

Kompetencje ministra właściwego do spraw informatyzacji wyznacza art. 12a ust. 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2025 r. poz. 1275), który obejmuje istotne z punktu widzenia niniejszej analizy sprawy:

1) informatyzacji administracji publicznej oraz podmiotów wykonujących zadania publiczne (art. 12a ust. 1 pkt 1 ustawy);

2) systemów i sieci teleinformatycznych administracji publicznej (art. 12a ust. 1 pkt 2 ustawy);

3) bezpieczeństwa cyberprzestrzeni w wymiarze cywilnym (art. 12a ust. 1 pkt 10 ustawy).

Zakres obowiązków ministra został jeszcze doprecyzowany w art. 45 ust. 1 pkt 11 ustawy o KSC poprzez nadanie mu uprawnienia do koordynowania *„działań organów państwa w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie niedotyczącej wymiaru militarnego"*. Tak ukształtowany zakres kompetencji ministra właściwego do spraw informatyzacji niewątpliwie obejmuje klasycznie rozumiane *ius politiae*, jako uprawnienie administracji publicznej do reagowania na sytuację zagrożenia bezpieczeństwa i porządku publicznego oraz zapobiegania tym zagrożeniom w zakresie w jakim nie wymaga to wprowadzenia któregoś ze stanów nadzwyczajnych (stanu klęski żywiołowej, stanu wyjątkowego bądź stanu wojennego).

W świetle powyższych przepisów zakres kompetencji ministra właściwego do spraw informatyzacji w obszarze bezpieczeństwa cyberprzestrzeni w wymiarze cywilnym obejmującym m.in. możliwość sprawowania nadzoru na tym obszarem, koordynowania działań administracji czy też prowadzenia działań w obszarze informatyzacji administracji nie budzi wątpliwości konstytucyjnych. W ocenie wnioskodawcy zastrzeżenia budzi natomiast przyznane w art. 67g ust. 1 ustawy o KSC uprawnienie ministra do wydawania aktu powszechnie obowiązującego o charakterze generalnym i abstrakcyjnym nazwanego poleceniem zabezpieczającym. Tak skonstruowany akt władczy nie mieści się w zamkniętym katalogu źródeł prawa określonym w art. 87 ust. 1 Konstytucji. W dotychczasowym orzecznictwie Trybunał Konstytucyjny podkreślał, że: *„Konstytucyjny system źródeł prawa ma charakter dualistyczny. Opiera się na podziale źródeł prawa na źródła prawa powszechnie obowiązującego (czemu dano wyraz w szczególności w art. 87 Konstytucji RP) i źródła prawa wewnętrznego (art. 93 Konstytucji RP). Potwierdzając rozwiązanie przyjęte przez ustrojodawcę, Trybunał Konstytucyjny w wyroku z 28.6.2000 r., K 25/99 (OTK 2000, Nr 5, poz. 141) wykluczył istnienie jakiejś trzeciej, pośredniej kategorii źródeł prawa."* – por. wyrok TK z dnia 12 grudnia 2011 r., sygn. akt P 1/11. Analogicznie Trybunał wypowiedział się w wyroku z dnia 10 lutego 2015 r., sygn. SK 50/13, wskazując, że: *„Katalog źródeł prawa powszechnie obowiązującego jest przy tym zamknięty. Konstytucja RP wyczerpująco wylicza formy aktów normatywnych powszechnie obowiązujących oraz podmioty upoważnione do ich wydawania (zob. np. wyr. TK z 28.6.2000 r., K 25/99, OTK 2000, Nr 5, poz. 141). Katalog źródeł prawa*

powszechnie obowiązującego został zamieszczony przede wszystkim w art. 87 ust. 1 i 2 Konstytucji RP. (...) W orzecznictwie Trybunału Konstytucyjnego ukształtowała się materialna koncepcja aktu normatywnego. Aktem normatywnym jest akt ustanawiający normy prawne o charakterze generalnym i abstrakcyjnym (zob. np.: orzecz. z 7.6.1989 r., U 15/88, OTK 1989, Nr 1, poz. 10; wyroki: z 16.11.2011 r., SK 45/09, OTK-A 2011, Nr 9, poz. 97; z 3.7.2012 r., K 22/09, OTK-A 2012, Nr 7, poz. 74). Generalność oznacza, że adresat określonej normy prawnej jest określony przez wskazanie określonej cechy lub cech rodzajowych. Natomiast abstrakcyjność „dotyczy przedmiotu normy określającego należne zachowanie się adresata. Przedmiotem normy prawnej winna być klasa zachowań się, nie zaś konkretne zachowanie się adresata. Konsekwencją abstrakcyjności normy jest (...) – to, że nie ulega umorzeniu czy «skonsumowaniu» poprzez jednorazowe zastosowanie" (zob. post. TK z 14.12.1999 r., U 7/99, OTK 1999, Nr 7, poz. 170).".

W świetle wskazanego powyżej sposobu wykładni art. 87 ust. 1 Konstytucji opierającego się na koncepcji zamkniętego katalogu źródeł prawa przewidziany przez ustawodawcę w art. 67g ust. 1, ust. 2, ust. 9 pkt 2, ust. 10 i ust. 11 ustawy o KSC akt władczy o charakterze generalnym i abstrakcyjnym, jakim jest polecenie zabezpieczające, w ogóle nie mieści się w tym katalogu źródeł prawa będących podstawą dla kształtowania praw i obowiązków podmiotów prawa w sposób powszechny. Okoliczność, iż akt ten wydawany jest w formie decyzji administracyjnej, w znacząco zmodyfikowanej procedurze administracyjnej (art. 67g ust. 3 ustawy o KSC przewiduje bowiem liczne wyłączenia w stosowaniu przepisów K.p.a. mających charakter gwarancji proceduralnych zabezpieczających prawa strony do rzetelnego postępowania administracyjnego) nie stoi na przeszkodzie w jego zakwalifikowaniu jako *sui generis* aktu normatywnego. O takim właśnie charakterze aktu przesądzają bowiem jego istotne cechy konstrukcyjne takie jak: zbiorowy adresat aktu, natychmiastowa wykonalność, publiczne obwieszczenie aktu zamiast jego indywidualnego doręczenia każdej ze stron, wyłączenie obowiązku udziału strony w postępowaniu administracyjnym, pozorność procedury dowodowej wobec wyłączenia ze stosowania kluczowych dla rzetelnego prowadzenia postępowania przepisów takich jak: art. 79, art. 81 czy art. 81a K.p.a.

Niezależnie od przedstawionych wyżej argumentów przemawiających za niezgodnością art. 67g ustawy o krajowym systemie cyberbezpieczeństwa z art. 87 ust. 1 Konstytucji, odrębnej oceny wymaga wpływ polecenia zabezpieczającego na konstytucyjnie chronioną sferę praw majątkowych jego adresatów. Wydanie przez ministra właściwego do spraw informatyzacji

polecenia zobowiązującego podmioty kluczowe oraz podmioty ważne do wykonania określonych nakazów lub zakazów może bowiem prowadzić do obciążenia tych podmiotów kosztami realizacji obowiązków publicznoprawnych, bez ustanowienia jakiegokolwiek mechanizmu ich rekompensaty.

Artykuł 64 ust. 2 Konstytucji ustanawia zasadę równej ochrony własności, innych praw majątkowych oraz prawa dziedziczenia. Ochrona ta przysługuje wszystkim podmiotom prawa, niezależnie od tego, czy prowadzą one działalność gospodarczą. Ustawodawca, nakładając obowiązki ingerujące w sferę majątkową określonych kategorii podmiotów, jest zatem zobowiązany ukształtować je w sposób respektujący konstytucyjny standard ochrony praw majątkowych oraz zachowujący właściwą proporcję między ciężarami nakładanymi na jednostkę a celem publicznym, któremu obowiązki te mają służyć.

Obowiązki nakładane na podstawie art. 67g ust. 1 oraz ust. 9 pkt 2 ustawy o krajowym systemie cyberbezpieczeństwa służą ograniczeniu skutków incydentu krytycznego albo zapobieżeniu jego rozprzestrzenianiu się. Realizacja tak określonego celu publicznego może jednak wymagać od adresatów polecenia poniesienia istotnych nakładów rzeczowych, organizacyjnych i osobowych. Ciężary te są przy tym nakładane w drodze jednostronnego rozstrzygnięcia organu władzy wykonawczej i mają być ponoszone wyłącznie przez podmioty objęte poleceniem, mimo że podejmowane działania służą ochronie dobra o charakterze ogólnym, jakim jest bezpieczeństwo systemów informacyjnych i ciągłość funkcjonowania państwa.

Wprawdzie art. 67g ust. 10 ustawy o krajowym systemie cyberbezpieczeństwa nie przewiduje bezpośrednio obowiązku wycofania z użytkowania sprzętu lub oprogramowania ICT pochodzącego od dostawcy uznanego za dostawcę wysokiego ryzyka, ponieważ skutek taki może wynikać z odrębnego rozstrzygnięcia wydawanego na podstawie art. 67b ust. 15 tej ustawy, nie oznacza to jednak, że wykonanie polecenia zabezpieczającego pozostaje neutralne dla sfery majątkowej jego adresatów. Już przed wydaniem decyzji w przedmiocie uznania danego podmiotu za dostawcę wysokiego ryzyka realizacja nakazów lub zakazów określonych w poleceniu może wymagać przeorganizowania procesów, zaangażowania dodatkowych zasobów, dokonania zmian technicznych albo czasowego ograniczenia korzystania z określonych rozwiązań ICT.

Ustawa nie przewiduje przy tym ani pełnej, ani choćby częściowej rekompensaty kosztów poniesionych w następstwie wykonania polecenia zabezpieczającego. W konsekwencji całość ekonomicznego ciężaru realizacji obowiązków służących ochronie interesu publicznego zostaje przeniesiona na ich adresatów, bez względu na wysokość

poniesionych nakładów, wpływ polecenia na prowadzoną działalność oraz stopień przyczynienia się danego podmiotu do powstania zagrożenia.

Takie ukształtowanie regulacji budzi zasadnicze zastrzeżenia z punktu widzenia art. 64 ust. 2 Konstytucji. Ustawodawca nie zapewnił bowiem mechanizmu pozwalającego na odpowiednie rozłożenie ciężarów wynikających z realizacji zadań służących ochronie bezpieczeństwa publicznego ani nie ustanowił instrumentów umożliwiających uwzględnienie rzeczywistych kosztów ponoszonych przez adresatów polecenia. Brak jakiejkolwiek regulacji kompensacyjnej może prowadzić do nieproporcjonalnego obciążenia ich majątku oraz do zróżnicowania zakresu ochrony praw majątkowych wyłącznie ze względu na objęcie określonego podmiotu reżimem ustawy o krajowym systemie cyberbezpieczeństwa.

W ocenie Wnioskodawcy pominięcie przez ustawodawcę mechanizmu rekompensowania kosztów ponoszonych w związku z wykonaniem polecenia zabezpieczającego prowadzi zatem do nieproporcjonalnej ingerencji w sferę praw majątkowych jego adresatów i pozostaje niezgodne ze standardem równej ochrony własności i innych praw majątkowych, wynikającym z art. 64 ust. 2 Konstytucji.

Jak wskazał Trybunał Konstytucyjny w wyroku z dnia 13 czerwca 2011 r., sygn. SK 41/09, *„(...) art. 64 ust. 2 Konstytucji RP formułuje podmiotowe prawo do równej dla wszystkich ochrony prawnej własności, innych praw majątkowych oraz prawa dziedziczenia. Jest to prawo podmiotowe w tym sensie, że nie tylko rodzi zobowiązanie ustawodawcy lub organu stosującego prawo do zapewnienia wszystkim równości wobec prawa, ale wyposaża podmioty w uprawnienie do żądania równej ochrony wymienionych w nim praw: własności, innych praw majątkowych i prawa dziedziczenia. Ścisłe powiązanie „równej dla wszystkich ochrony prawnej" z prawem do własności, innymi prawami majątkowymi i prawem dziedziczenia powoduje, że tak pojmowana równość staje się jego nieodłącznym aspektem, bez którego prawa z art. 64 ust. 2 Konstytucji RP pozbawione zostałyby swojej istoty. Równość, o której mowa w art. 64 ust. 2 Konstytucji RP, nie ma zatem charakteru abstrakcyjnego. Odnosi się do konkretnych, wymienionych w tym przepisie praw i do zapewnienia im takiej właśnie, to jest równej ochrony (...).".*

W świetle powyższych zastrzeżeń, na tle całości regulacji zawartej w art. 67g ustawy o KSC możliwe jest też sformułowanie kolejnego zarzutu względem samej procedury wydawania polecenia zabezpieczającego przez ministra właściwego do spraw informatyzacji i to niezależnie od podniesionych powyżej zastrzeżeń co do charakteru prawnego polecenia zabezpieczającego. Nierzetelność postępowania administracyjnego godzi bowiem wprost w

zasadę państwa prawnego (art. 2) oraz zasadę legalizmu działania organów administracji (art. 7). Należy wskazać, że ograniczenia gwarancji rzetelnego postępowania administracyjnego w postępowaniu w sprawie o wydanie polecenia zabezpieczającego wynikają z art. 67g ust. 3 ustawy o KSC, który wprost wyłącza stosowanie poniższych przepisów K.p.a.:

1) art. 10 – zasada czynnego udziału strony w postępowaniu;

2) art. 34 – obowiązek zapewnienia przez organ właściwej reprezentacji dla strony nieobecnej lub niezdolnej do czynności prawnych;

3) art. 79 – obowiązek zapewnienia stronie czynnego udziału w postępowaniu dowodowym;

4) art. 81 – możliwość wypowiedzenia się przez stronę odnośnie przeprowadzonych dowodów;

5) art. 81a – obowiązek rozstrzygania wątpliwości na korzyść strony;

6) art. 107 § 1 pkt 3 – obowiązek oznaczenia w decyzji strony postępowania;

7) art. 145 § 1 pkt 4 – możliwość wznowienia postępowania z uwagi na brak udziału w postępowaniu;

8) art. 156 § 1 pkt 4 – możliwość stwierdzenia nieważności postępowania, jeżeli decyzja została skierowana do osoby niebędącej stroną postępowania;

9) rozdziału 8 działu I K.p.a., tj. art. 39 – art. 49b w zakresie wyłączenia stosowania zasady oficjalności doręczeń.

W świetle zastosowanych przez ustawodawcę kilkunastu wyłączeń w stosowaniu Kodeksu postępowania administracyjnego oraz po nałożeniu na ministra właściwego do spraw informatyzacji obowiązku „odpowiedniego stosowania" całości K.p.a. w zakresie w jakim nie został on wyłączony w art. 67g ust. 3 ustawy o KSC powstaje zasadnicze pytanie czy w świetle art. 2 i art. 7 Konstytucji, jako konstytucyjnych wzorców oceny, w ogóle możliwe jest funkcjonowanie tak ukształtowanej procedury przygotowywania i wydawania polecenia zabezpieczającego, która z jednej strony wyłącza ze stosowania przez organ istotne elementy procedury administracyjnej, a z drugiej strony wydany w ten sposób akt władczy nosi wszelkie znamiona aktu normatywnego (o czym była mowa powyżej). Jak wskazał Trybunał Konstytucyjny w wyroku z dnia 16 marca 2011 r., sygn. K 35/08, *„Obowiązkiem prawodawcy jest określenie zarówno podstaw, jak i granic działania organów władzy. Kompetencje organów władzy publicznej mogą być, w zależności od charakteru sprawy, określone bardziej lub mniej szczegółowo, lecz ich przyznanie jest warunkiem koniecznym legalnego działania tych organów. Prawodawca nie może przy tym dowolnie przydzielać kompetencji poszczególnym*

organom, ale powinien to czynić, mając na uwadze „rolę i pozycję ustrojową danego organu" (zob. wyr. z 23.3.2006 r., K 4/06, OTK-A 2006, Nr 3, poz. 32).".

W ocenie Wnioskodawcy zakres kompetencji przyznanych ministrowi właściwemu do spraw informatyzacji, obejmujących możliwość wydawania polecenia zabezpieczającego wywołującego skutki wobec nieoznaczonego kręgu adresatów, wykracza poza konstytucyjnie określoną pozycję ustrojową ministra kierującego działem administracji rządowej. Zgodnie z art. 149 ust. 1 Konstytucji minister kieruje określonym działem administracji rządowej albo wypełnia zadania wyznaczone mu przez Prezesa Rady Ministrów. Przepis ten nie daje natomiast podstaw do wyposażenia ministra w kompetencję do kształtowania w sposób generalny i abstrakcyjny sytuacji prawnej podmiotów pozostających poza strukturą organizacyjną kierowanego przez niego działu administracji rządowej.

Polecenie zabezpieczające, z uwagi na zakres jego oddziaływania oraz sposób określenia kręgu podmiotów nim związanych, nie ogranicza się do sfery kierownictwa, nadzoru lub podległości organizacyjnej właściwej dla relacji zachodzących w ramach administracji rządowej. Może ono bowiem ingerować także w sytuację prawną podmiotów niepozostających w stosunku podległości służbowej ani organizacyjnej wobec ministra. W rezultacie kompetencja ta przybiera cechy władczego oddziaływania o charakterze powszechnym, wykraczającego poza konstytucyjnie dopuszczalny zakres działania organu administracji rządowej.

Zastrzeżenia konstytucyjne potęguje okoliczność, że polecenie zabezpieczające, mimo jego generalnego zakresu oddziaływania, ma być wydawane w trybie administracyjnym pozbawionym zasadniczych gwarancji służących zapewnieniu rzetelności postępowania oraz skutecznej ochrony praw adresatów ingerencji. Tak ukształtowana procedura nie zapewnia dostatecznej ochrony przed arbitralnością działania organów władzy publicznej i pozostaje w sprzeczności z zasadą demokratycznego państwa prawnego wyrażoną w art. 2 Konstytucji oraz z zasadą legalizmu wynikającą z art. 7 Konstytucji.

Zasada legalizmu wymaga, aby kompetencje organów władzy publicznej, przesłanki ich wykonywania oraz tryb podejmowania rozstrzygnięć zostały określone w sposób dostatecznie precyzyjny i odpowiadający ustrojowej pozycji danego organu. Ustawodawca nie może zatem kształtować kompetencji ministra w sposób prowadzący do zatarcia granicy między

stosowaniem prawa a stanowieniem norm o charakterze generalnym i abstrakcyjnym. Minister właściwy do spraw informatyzacji pozostaje organem władzy wykonawczej, którego zadaniem jest wykonywanie ustaw, nie zaś ustanawianie – w formie nieprzewidzianej w Konstytucji – norm powszechnie wiążących podmioty pozostające poza zakresem jego kierownictwa lub nadzoru.

Za nieuzasadnione należy również uznać przyjęcie, że zakwalifikowanie określonych podmiotów jako podmiotów kluczowych albo podmiotów ważnych w rozumieniu załączników nr 1 i 2 do ustawy o krajowym systemie cyberbezpieczeństwa prowadzi do osłabienia przysługujących im gwarancji konstytucyjnych. Sam fakt objęcia określonego podmiotu szczególnym reżimem prawnym ze względu na znaczenie wykonywanej przez niego działalności nie oznacza ograniczenia standardu ochrony jego praw, autonomii organizacyjnej i majątkowej ani prawa do skutecznego kwestionowania ingerencji organów władzy publicznej. Samo istnienie ryzyka wystąpienia incydentów dotyczących systemów informacyjnych, w tym incydentów krytycznych w rozumieniu art. 2 pkt 6 ustawy o krajowym systemie cyberbezpieczeństwa, nie może stanowić wystarczającego uzasadnienia dla ustanowienia instrumentów prawnych prowadzących do daleko idącej ingerencji w sferę działalności podmiotów prawa oraz w przyjęty przez nie sposób zarządzania incydentami. Ingerencja taka powinna pozostawać w zgodzie z zasadą proporcjonalności, być niezbędna dla ochrony konstytucyjnie legitymowanego celu oraz zostać obudowana odpowiednimi gwarancjami materialnymi i proceduralnymi.

Ingerencja ustawodawcza w tym zakresie powinna pozostawać w zgodzie z konstytucyjnymi standardami ochrony autonomii podmiotów prawa, ich samodzielności organizacyjnej i majątkowej, a także gwarantować im możliwość skutecznej ochrony przysługujących praw i interesów prawnych. Niedopuszczalne jest zatem kształtowanie instrumentów prawnych w sposób prowadzący do nadmiernego ograniczenia swobody decyzyjnej tych podmiotów lub pozbawiający je realnych środków kwestionowania rozstrzygnięć ingerujących w ich sferę prawną.

Obowiązkiem ustawodawcy jest ustanowienie takich mechanizmów prawnych, które zapewnią należytą ochronę bezpieczeństwa państwa i ciągłości funkcjonowania jego istotnych struktur, a zarazem będą respektowały zasadę proporcjonalności oraz autonomię podmiotów korzystających z legalnie dostępnych na rynku rozwiązań technicznych.

W związku z powyższym konieczne jest zbadanie zgodności z Konstytucją wskazanych w *petitum* wniosku przepisów przez Trybunał Konstytucyjny jako jedyny organ władzy publicznej powołany do tej funkcji z mocy Konstytucji Rzeczypospolitej Polskiej.