

2025-12-04 13:23

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU

L. dz. SPS-III.020.368.M.2025

Data wpływu 05.XII.25r.

Szanowny Panie Marszałku, Szanowni Państwo,

Mając na uwadze procedowany aktualnie przez Prawodawcę Druk Sejmowy nr 1955 pozwalam sobie przesłać w załączeniu *polemiczną* opinię dotyczącą tego projektu, która to opinia stanowi wycinek większej pracy naukowej nad którą aktualnie pracuję w ramach Wydziału Prawa i Administracji Uniwersytetu Warszawskiego (gdzie prowadzę zajęcia i prace naukowe dotyczące e-administracji i cyberbezpieczeństwa).

Z wyrazami głębokiego szacunku

prof. Paweł Wajda (adwokat)
Wydział Prawa i Administracji
Uniwersytet Warszawski
T.:
E.: p.wajda@wpia.uw.edu.pl

OPINIA NA ZASADZIE *AMICUS CURIAE*
DOTYCZĄCA PROJEKTU USTAWY O ZMIANIE USTAWY O KRAJOWYM
SYSTEMIE CYBERBEZPIECZEŃSTWA

Warszawa, dnia 03 grudnia 2025 r.

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU

L. dz. SPS-III. QO. 368. 11. 2025

Data wpływu 05. XII. 25r.

I. Przedmiot opinii.

1. Kierując się troską o zapewnienie prawidłowej, proporcjonalnej i zgodnej z zasadami techniki legislacyjnej implementacji prawa Unii Europejskiej do krajowego porządku prawnego, a także wyrażając - jako osoba zajmująca się naukowo tematyką e-administracji oraz cyberbezpieczeństwa, prowadząca w tej tematyce zajęcia akademickie i publikująca prace naukowe, jak np. publikacja: Cyberbezpieczeństwo – sektorowe aspekty regulacyjne - internetowy Kwartalnik Antymonopolowy i Regulacyjny - Volume 9, Issue 2 (2020) - CEJSH - Yadda) - uzasadnione zaniepokojenie kierunkiem, w jakim zmierza aktualnie procedowany przez Sejm Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Druk nr 1955¹; dalej: „Projekt Ustawy”), przedstawiam niniejszą opinię *amicus curiae*.
2. Niniejsza opinia na zasadzie *amicus curiae* stanowi wyraz obawy, że Projekt Ustawy w zakresie, w szczególności projektowanych przepisów z art. 67b i nast. Projektu Ustawy - niezależnie od słuszných intencji ochronnych, które mogą mu przyświecać - prowadzi do ingerencji w sferę wolności działalności gospodarczej w stopniu wykraczającym zarówno poza standard dopuszczalny na gruncie prawa krajowego, jak i poza zakres wynikający z 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 NIS2)², której wdrożeniu nowelizacji Projekt Ustawy ma służyć. W rezultacie projektowana regulacja zdaje się wprowadzać rozwiązania, które w sposób nieproporcjonalny oraz nieuprawniony rozszerzają obowiązki adresatów norm prawnych, a więc stanowią klasyczną postać tzw. *gold-platingu*.
3. Niniejsza opinia na zasadzie *amicus curiae* ma na celu zwrócenie uwagi prawodawcy na te fragmenty Projektu Ustawy, które - w mojej ocenie - prowadzą do nieuzasadnionego i pionowo niezgodnego z porządkiem unijnym oraz krajowym wzmocnienia zakresu obowiązków nakładanych na uczestników obrotu, zobowiązanych do stosowania przepisów przewidzianych w Projekcie Ustawy i znaczną nowelizujących dotychczasową treść ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa³. Wzmacnianie to przybiera postać nadregulacji, polegającej na konstruowaniu obowiązków wykraczających poza standard minimalny wynikający z prawa Unii Europejskiej, i jednocześnie - poprzez swój ciężar i rozległość - tworzy mechanizmy, które mogą naruszać

¹ Treść rządowego projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Druk nr 1955) dostępna jest na stronie internetowej pod adresem: <https://www.sejm.gov.pl/sejm10.nsf/druk.xsp?nr=1955> (data dostępu: 02.12.2025 r.).

² Dz. Urz. UE L 333 z 27.12.2022 r., str. 80; dalej: „Dyrektywa NIS2”.

³ Tekst jednolity: Dz. U. z 2024 r. poz. 1077 ze zm.

przepisy konstytucyjne, w tym zasadę proporcjonalności oraz wywoływać efekt nadmiernej restrykcyjności w relacji państwo-przedsiębiorca.

4. W tym kontekście szczególnie istotne jest podkreślenie, że najbardziej doniosłe wątpliwości konstytucyjne budzą przepisy art. 67b i nast. Projektu Ustawy. To one stanowią rdzeń mechanizmu uznawania dostawców ICT za podmioty „wysokiego ryzyka” oraz określają daleko idące konsekwencje takiej kwalifikacji, w tym obowiązek usunięcia sprzętu i oprogramowania z użytkowania, zakaz ich dalszego nabywania oraz wynikające z tego ciężary ekonomiczne i organizacyjne. To właśnie te regulacje - poprzez swój zakres, intensywność ingerencji i systemowe skutki - prowadzą do najsilniejszego napięcia między Projektowaną Ustawą a konstytucyjnymi zasadami proporcjonalności, rzetelności procesu prawotwórczego, ochrony własności oraz społecznej gospodarki rynkowej. W szczególności tworzą one rozwiązania, które w sposób pionowy rozmiągają się z Konstytucją Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.⁴, naruszając zarówno jej postanowienia materialne, jak i proceduralne, co budzi moje szczególne zaniepokojenie.
5. Aby prawidłowo ocenić projektowaną regulację, konieczne jest odniesienie jej do ugruntowanych w doktrynie oraz orzecznictwie zasad ograniczania wolności działalności gospodarczej. W literaturze prawa publicznego podkreśla się, że ingerencja ustawodawcy w sferę aktywności gospodarczej musi mieścić się w ramach konstytucyjnych i europejskich w taki sposób, aby nakładane obowiązki nie przekraczały minimalnej intensywności koniecznej do realizacji zakładanych celów regulacyjnych. Zasada proporcjonalności - rozumiana szeroko, jako obejmująca wymogi konieczności, przydatności i minimalności środka - pełni tu funkcję kluczowego filtra oceny legislacyjnej. Równocześnie znaczenie ma zasada ochrony zaufania uczestników rynku, która wymaga, aby podmioty prowadzące działalność gospodarczą mogły w przewidywalny sposób ocenić następstwa prawne swoich działań.
6. Nadmierna ingerencja ustawodawcy, wykraczająca poza treść przepisów unijnych, tworzy bowiem ryzyko zastępowania norm o jasno określonym charakterze obowiązującymi *implicite* standardami interpretacyjnymi, co prowadzi do zacierania granicy pomiędzy obowiązkiem wynikającym z prawa a oczekiwaniami organów państwa⁵. W szerokiej perspektywie teoretycznej, rozwiniętej w doktrynie prawa regulacyjnego - w tym w analizach odnoszących się do szeregu rynków regulowanych, również tych o znacznym stopniu infrastrukturalności i wrażliwości społeczno-ekonomicznej - wskazuje się, że nadmierna intensywność regulacji może w praktyce prowadzić do kształtowania nowych modeli funkcjonowania danego sektora.

⁴ Dz. U. Nr 78, poz. 483 ze zm.

⁵ Por. np.: L. Squintani, *Gold-Plating: A Misleading Overarching Concept*, w: L. Squintani (red.), *Beyond Minimum Harmonisation: Gold-Plating and Green-Plating of European Environmental Law*, Cambridge: Cambridge University Press 2019, s. 33.

7. W doktrynie prawa Unii Europejskiej akcentuje się ponadto, że zbyt daleko idące rozszerzanie obowiązków na etapie implementacji dyrektyw unijnych wypacza sens harmonizacji minimalnej, przekształcając ją w harmonizację maksymalną o charakterze lokalnym, a tym samym zakłócając równe warunki działania przedsiębiorców w ramach rynku wewnętrznego. W rezultacie państwo członkowskie Unii Europejskiej - niejako wbrew celom dyrektywy unijnej - tworzy system bardziej restrykcyjny niż ten przewidziany przez prawodawcę unijnego, co stanowi naruszenie zasady lojalnej współpracy i podważa spójność europejskiego porządku prawnego.
8. Przedmiotowy Projekt Ustawy wykazuje cechy tego rodzaju nadmiernej rozbudowy regulacyjnej. W wielu miejscach wprowadza on bowiem obowiązki o charakterze publicznoprawnym bądź *quasi*-penalnym, które nie wynikają z Dyrektywy NIS2, a są efektem nadbudowania jej przepisów przez prawodawcę krajowego. Prowadzi to do ukształtowania systemu odpowiedzialności, w którym istotą nie staje się naruszenie precyzyjnie określonego obowiązku, lecz niespełnienie standardów, które można określić jako domniemane bądź wyinterpretowane na podstawie ogólnej intencji regulacyjnej⁶.
9. Konsekwencją takich rozwiązań jest naruszenie zasady proporcjonalności, wykraczanie poza dopuszczalny zakres harmonizacji oraz wprowadzanie znaczącej niepewności regulacyjnej. Zjawisko to generuje poważne ryzyka dla stabilności otoczenia prawnego sektorów o wysokim stopniu regulacji, a tym samym również dla przewidywalności i bezpieczeństwa prowadzenia działalności gospodarczej dla podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa.
10. W tym kontekście celem niniejszej opinii na zasadzie *amicus curiae* jest przedstawienie pogłębionej analizy tych elementów Projektu Ustawy, które - jak się wydaje - nie znajdują odpowiedniego oparcia ani w prawie unijnym, ani w prawie krajowym, a których przyjęcie mogłoby prowadzić do stosowania nieproporcjonalnych środków ingerencji w działalność gospodarczą podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa. W niniejszej opinii na zasadzie *amicus curiae* wskazano dlaczego przedstawione poniżej rozwiązania pozostają w kolizji z zasadami prawidłowej legislacji, w tym z zasadą przejrzystości i pewności prawa, oraz dlaczego ich implementacja mogłaby skutkować powstaniem instrumentów odpowiedzialności administracyjnej lub nawet *quasi*-karnej, niewspółmiernej do celu regulacji i niewynikającej z jednoznacznie przewidzianych w prawie obowiązków.
11. Niniejsza opinia na zasadzie *amicus curiae* ma charakter konstruktywny i służy temu, aby wesprzeć proces legislacyjny w dążeniu do rozwiązań, które będą zgodne z zasadami

⁶ Por. szerzej: Wyrok NSA z dnia 13 lutego 2014 r.; sygnatura: II GSK 1923/12; LEX nr 1450720; por. także: Wyrok WSA w Warszawie z dnia 12 lipca 2012 r.; sygnatura: VI SA/Wa 159/12; LEX nr 1230739; Wyrok NSA z dnia 13 lutego 2014 r.; sygnatura: II GSK 1923/12; LEX nr 1450720 Wyrok WSA w Warszawie z dnia 27 lipca 2016 r.; sygnatura: VI SA/Wa 132/16; LEX nr 2137912; Wyrok WSA w Warszawie z dnia 12 grudnia 2019 r.; sygnatura: VI SA/Wa 641/19; LEX nr 3014572.

sprawiedliwości, proporcjonalności, racjonalnej regulacji sektorowej oraz adekwatnej implementacji prawa Unii Europejskiej do polskiego porządku prawnego. Jednocześnie jej celem jest wskazanie tych elementów Projektu Ustawy, które warto - z perspektywy zarówno zgodności systemowej, jak i pewności obrotu - poddać ponownej weryfikacji przez polskiego ustawodawcę oraz adekwatnej ocenie i rewizji ostatecznego tekstu Projektu Ustawy.

II. Executive Summary.

Dokonana analiza prawna doprowadziła do sformułowania następujących konkluzji:

- (1) Dokonana analiza Projektu Ustawy, w zakresie mechanizmu uznawania dostawcy ICT za „dostawcę wysokiego ryzyka” (art. 67b i nast. Projektu Ustawy), prowadzi do jednoznacznego wniosku, że mechanizm ten stanowi daleko idącą ingerencję w wolność działalności gospodarczej, prawo własności oraz gwarancje proceduralne, a zatem – jako środek prawa publicznego – musi być zgodny zarówno z prawem UE (Dyrektywa NIS2, TFUE i KPP), jak i Konstytucją RP. Taka zgodność nie została wykazana.
- (2) Procedura kwalifikacyjna opiera się na szerokim uznaniu administracyjnym ministra i niedookreślonych przesłankach oceny ryzyka, przy czym decyzja ma skutek generalny, jest natychmiast wykonalna i obejmuje całą grupę kapitałową oraz liczne produkty/usługi ICT. Oczywistą konsekwencją tej konstrukcji jest istotne osłabienie gwarancji procesowych i faktyczne ograniczenie prawa do sądu.
- (3) Nakładane obowiązki - w tym nakaz wycofania z użytkowania oraz zakaz nabywania określonych produktów ICT w terminach 4-7 lat - obciążają podmioty kluczowe, ważne oraz przedsiębiorców telekomunikacyjnych. Projekt nie przewiduje przy tym jakiejkolwiek kompensacji z tytułu przymusowego usunięcia infrastruktury. Konsekwencją takiego braku jest powstanie regulacji o charakterze *quasi*-wywłaszczeniowym, sprzecznej z art. 21 i art. 64 Konstytucji RP oraz z zasadą proporcjonalności (ujętą w treści art. 31 ust. 3 Konstytucji RP).
- (4) Projekt dokonuje niedopuszczalnej nadtranspozycji (*gold-platingu*). Dyrektywa NIS2 ma charakter minimalnej harmonizacji; państwo może zaostrzać regulacje jedynie pod warunkiem zachowania proporcjonalności, subsydiarności, transparentności i braku barier dla rynku wewnętrznego Unii Europejskiej. Warunki te nie zostały spełnione, gdyż Projekt implementuje zalecenia *soft law* (5G Toolbox) jako normy wiążące oraz przewiduje sankcje i restrykcje wykraczające poza standard UE.
- (5) Ustawodawca krajowy - aby móc wprowadzić nadstandardowe środki w procesie implementacji dyrektywy unijnej - musi wykazać ich niezbędność, przydatność i adekwatność. Tymczasem Projekt Ustawy nie przedstawia sektorowych ocen ryzyka, nie zawiera dowodów konieczności środków oraz nie przewiduje alternatyw mniej dolegliwych. Oczwistym jest więc, że zabrakło elementarnego wymogu „evidence-based regulation”.
- (6) Implementacja dokonana w Projekcie Ustawy pozostaje w sprzeczności z prawem Unii Europejskiej. *Soft law* nadano skutek wiążący i rozciągnięto je na wszystkie sektory, do których zastosowanie znajdzie Dyrektywa NIS2, wprowadzając środki definitywne (nakazy wycofania, zakazy wprowadzania), podczas gdy dyrektywa

przewiduje podejście sekwencyjne i ryzykobazowe. Konsekwencją tego jest naruszenie zasad jednolitego rynku, swobody przedsiębiorczości, swobody świadczenia usług oraz prawa własności.

- (7) Konstrukcja proceduralna Projektu Ustawy - wyłączenia k.p.a., ograniczenia kręgu stron, natychmiastowa wykonalność decyzji oraz doręczanie wyłącznie niejawniej części uzasadnienia - kumulatywnie narusza zasadę legalizmu, zasadę rzetelności legislacyjnej oraz prawo do sądu. Nie może być bowiem efektywnej kontroli sądowej tam, gdzie organ pozbawia stronę pełnego dostępu do akt i uzasadnienia.**
- (8) Wprowadzenie poleceń zabezpieczających oraz możliwości quasi-automatycznego zawieszania i cofania koncesji - bez wcześniejszej analizy ryzyka i bez realnej kontroli merytorycznej - stanowi ingerencję nieproporcjonalną i sprzeczną z art. 87 ust. 1 Konstytucji RP, podważającą system źródeł prawa.**
- (9) Porównanie rozwiązań przyjętych w państwach UE jednoznacznie wskazuje, że Polska przyjęła model najdalej idący, obejmujący wszystkie 18 sektorów NIS2 oraz 38-40 tys. adresatów, bez zróżnicowania względem krytyczności usług. Jest to przypadek skrajnego, niedopuszczalnego gold-platingu, prowadzący do fragmentacji rynku wewnętrznego oraz nierówności konkurencji.**

III. Analiza prawna.

III.1. Przepisy Projektu Ustawy stanowiące przedmiot niniejszej analizy prawnej.

1. W pierwszym kroku należy kategorycznie wskazać, że przedmiotem niniejszej opinii na zasadzie *amicus curiae* będzie analiza mechanizmu dostawcy wysokiego ryzyka przewidzianego w Projekcie Ustawy, w tym ocena jego zgodności z prawem Unii Europejskiej, w szczególności z Dyrektywą NIS2, Traktatem o Funkcjonowaniu Unii Europejskiej (TFUE)⁷ oraz Kartą Praw Podstawowych Unii Europejskiej⁸, a także z Konstytucją RP, w tym w zakresie swobody przepływu towarów, swobody przedsiębiorczości, wolności prowadzenia działalności gospodarczej, prawa własności, zasady proporcjonalności oraz standardów proceduralnych.
2. Warto w tym miejscu przytoczyć przepisy będące przedmiotem oceny w treści niniejszej opinii na zasadzie *amicus curiae*. I tak kluczowym przepisem ujętym w treści Projektu Ustawy, który budzi istotne wątpliwości w zakresie jego zgodności z przepisami Konstytucji RP oraz przepisami prawa Unii Europejskiej jest mechanizm uznania dostawcy za podmiot wysokiego ryzyka, przewidziany w art. 67b Projektu Ustawy, który należy do regulacji najbardziej problematycznych, ponieważ prowadzi do arbitralnego i asymetrycznego przerzucenia ciężarów publicznych na podmioty prywatne, i to bez gwarancji należytej ochrony ich praw.

Zgodnie z aktualnie projektowanym brzmieniem przepisu z art. 67b Projektu Ustawy: *1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć, z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania, które są wykorzystywane przez:*

- 1) podmioty kluczowe lub podmioty ważne, z wyłączeniem podsektora komunikacji elektronicznej,*
 - 2) przedsiębiorców komunikacji elektronicznej, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych,*
 - 3) podmioty finansowe, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554*
- za dostawcę wysokiego ryzyka.*

⁷ Traktat uzupełniony Protokołem w sprawie przywilejów i immunitetów Unii Europejskiej (Dz.U.04.90.864/4) w związku ze zmianami wprowadzonymi do tegoż protokołu przez art. 1 pkt 3 lit. a) Protokołu nr 1 zmieniającego protokoły dołączone do Traktatu o Unii Europejskiej, Traktatu ustanawiającego Wspólnotę Europejską lub Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej dołączonego do Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (Dz.U.U.E.C.07.306.1) z dniem 1 grudnia 2009 r.; dalej: „TFUE”.

⁸ Dz. U. UE. C. z 2016 r. Nr 202, str. 389; dalej: „Karta Praw Podstawowych”.

2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, jeżeli ustawa nie stanowi inaczej, stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy.
3. Stroną postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest każdy, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka.
4. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka może przystąpić, na wniosek, na prawach strony, przedsiębiorca telekomunikacyjny mający siedzibę na terytorium Rzeczypospolitej Polskiej wpisany do rejestru przedsiębiorców telekomunikacyjnych, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2024 r. poz. 1631 i 1674 oraz z 2025 r. poz. 718, 769 i 1159). Przepisy art. 31 § 2 i 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio.
5. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego ogłoszony przed wszczęciem postępowania.
6. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Zawiadomienie publikuje się także na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, niezwłocznie po doręczeniu tego zawiadomienia.
7. Minister właściwy do spraw informatyzacji zawiadamia Prokuratora Generalnego o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka.
8. Jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym zawiadomienie, o którym mowa w ust. 6, publikuje się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. Udostępnienie ma skutek doręczenia zawiadomienia stronie po upływie 14 dni od dnia jego dokonania.
9. W terminie 14 dni od dnia opublikowania na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji zawiadomienia, o którym mowa w ust. 6 i 8, organizacja społeczna może przedstawić ministrowi właściwemu do spraw informatyzacji stanowisko co do dostawcy sprzętu lub oprogramowania, wobec którego

wszczęto postępowanie, oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT. Minister właściwy do spraw informatyzacji, przed wydaniem decyzji, publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej raport ze złożonych w terminie stanowisk, wskazując w szczególności główne uwagi zawarte w stanowiskach.

10. Przed wydaniem decyzji minister właściwy do spraw informatyzacji zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do Kolegium do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

11. Opinia, o której mowa w ust. 10 zdanie pierwsze, zawiera analizę:

1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich Unii Europejskiej lub organów Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;

2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:

a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie,

b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności w przypadku, gdy nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem,

c) struktury własnościowej dostawcy sprzętu lub oprogramowania,

d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;

3) powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.05.2019, str. 1, z późn. zm.));

4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;

5) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o

których mowa w ust. 1, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;

6) treści wydanych rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy.

12. Sporządzając opinię, o której mowa w ust. 10 zdanie pierwsze, Kolegium uwzględnia:

1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, w szczególności certyfikaty wydane w ramach europejskich programów certyfikacji cyberbezpieczeństwa;

2) analizy, o których mowa w art. 65a ust. 1 i 2.

13. Procedura sporządzenia opinii, o której mowa w ust. 10 zdanie pierwsze, przebiega w następujący sposób:

1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym”, w skład którego wchodzi przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium;

2) każdy członek zespołu opiniującego przygotowuje stanowisko, w zakresie swojej właściwości, które następnie przekazuje zespołowi opiniującemu. W przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium, wskazując właściwego członka zespołu opiniującego;

3) jeżeli nie zostały wykonane analizy, o których mowa w art. 65a ust. 1 i 2, przewodniczący Kolegium zleca ich wykonanie;

4) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii;

5) ustalenie opinii następuje na posiedzeniu Kolegium;

6) ustaloną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.

14. W zespole opiniującym może wziąć udział również przedstawiciel Prezesa Urzędu Ochrony Konkurencji i Konsumentów. W posiedzeniu Kolegium, na którym następuje ustalenie opinii, może wziąć udział Prezes lub Wiceprezes Urzędu Ochrony Konkurencji i Konsumentów.

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.

17. Minister właściwy do spraw informatyzacji ogłasza decyzję, o której mowa w ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz publikuje na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra.

18. Decyzja, o której mowa w ust. 15, podlega natychmiastowemu wykonaniu.

19. Od decyzji, o której mowa w ust. 15, nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

3. Decyzja ministra - oparta na otwartych, szeroko zakreślonych kryteriach, które nie zawierają wymogu przeprowadzenia analizy proporcjonalności ani wykazania niezbędności środka - prowadzi do natychmiastowych skutków gospodarczych o charakterze powszechnym i generalnym. Zakaz wprowadzania na rynek określonych produktów, nakaz ich usunięcia w ciągu czterech do siedmiu lat oraz ograniczenia dotyczące dalszego nabywania sprzętu lub oprogramowania nie stanowią zwykłej regulacji technicznej, lecz ingerują w samą istotę prawa własności i wolności działalności gospodarczej. W rezultacie efekty decyzji z art. 67b Projektu Ustawy są funkcjonalnie równoważne z wywłaszczeniem⁹, przy czym Projekt Ustawy nie przewiduje żadnego mechanizmu kompensacyjnego, co - zgodnie z mają najlepszą wiedzę - pozostaje w sprzeczności z art. 21 ust. 2 Konstytucji RP i związanym z nim standardem ochrony własności, wskazanej w przepisie z art. 64 Konstytucji RP.
4. Naruszona – co zostanie wykazane w treści niniejszej opinii na zasadzie *amicus curiae* - zostaje także zasada proporcjonalności w jej wymiarze formalnym i materialnym, wynikająca z art. 31 ust. 3 Konstytucji RP. Środek tak drastyczny jak generalny zakaz użytkowania danego typu technologii może zostać wprowadzony wyłącznie wtedy, gdy jest konieczny, przydatny i najmniej dolegliwy spośród dostępnych, a jednocześnie gdy państwo przeprowadzi rzetelną ocenę ryzyka i wykaże niemożność zastosowania narzędzi mniej restrykcyjnych.

⁹ M. Safjan, L. Bosek (red.), *Konstytucja RP. Tom I. Komentarz do art. 1-86*, Warszawa 2016; Wyrok TK z dnia 12 kwietnia 2000 r.; sygnatura: K 8/98; Legalis; Wyrok TK z dnia 16 czerwca 2015 r.; sygnatura: K 25/12; Legalis; Wyrok NSA z dnia 13 lipca 2021 r.; sygnatura: I OSK 2367/20; LEX nr 3198087; tak też: P. Tuleja [w:] P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radziejewicz, P. Tuleja, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2023, art. 21.

5. Tymczasem środki, które obecnie istnieją w unijnym i krajowym porządku prawnym - takie jak certyfikacja cyberbezpieczeństwa¹⁰, kontrola zgodności, środki zarządzania ryzykiem, testy penetracyjne, audyty czy obowiązki sprawozdawcze - są ignorowane na rzecz instrumentu ostatecznego, ingerującego w strukturę rynku i w autonomię podmiotów gospodarczych. Prawodawca pomija także Dyrektywę NIS2, która wymaga, aby środki stosowane przez państwa członkowskie były proporcjonalne i adekwatne do rzeczywistego ryzyka, co dodatkowo potęguje wrażenie nadregulacji i braku racjonalności prawodawczej.
6. Niepokój budzi ponadto konstrukcja progów uczestnictwa w postępowaniu przewidziana w art. 67b ust. 1 i ust. 4 Projekt Ustawy. Przewidując ograniczenie możliwości udziału w sprawie jedynie do podmiotów przekraczających określone progi przychodowe, ustawodawca narusza zasadę równości proceduralnej oraz zasadę przyzwoitej legislacji, wynikającą z art. 2 Konstytucji RP. Podmioty, które będą zobowiązane do ponoszenia realnych kosztów wymiany sprzętu czy oprogramowania, nie będą mogły brać udziału w postępowaniu, które decyduje o ich obowiązkach. Wyłączenie ich z udziału w sprawie jest nie tylko nieuzasadnione konstytucyjnie, ale również sprzeczne z zasadą ochrony zaufania obywateli do państwa, ponieważ ustawodawca tworzy sytuację, w której przedsiębiorca ponosi ciężary wynikające z decyzji, na którą nie miał wpływu i której nie mógł zakwestionować w ramach standardowej procedury.
7. Szczególne zastrzeżenia budzi również sposób ukształtowania postępowania administracyjnego, w tym wyłączenia stosowania szeregu kluczowych przepisów ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego¹¹. Wyłączenia te obejmują między innymi art. 28 k.p.a., stanowiący fundament dla określenia statusu strony postępowania, oraz przepisy dotyczące dowodów, rozprawy administracyjnej i prawa do wglądu w akta. Odbiera to przedsiębiorcom gwarancje procesowe niezbędne do ochrony ich praw i interesów, a tym samym narusza art. 2 Konstytucji RP, w którym wyrażony jest nakaz rzetelnego i sprawnego działania organów władzy publicznej. Tak dalekie ograniczenie gwarancji procesowych wykracza poza konstytucyjnie dopuszczalne ramy ingerencji w prawa jednostki i nie znajduje uzasadnienia nawet w sytuacjach wymagających wzmożonej ochrony bezpieczeństwa państwa¹².
8. Nie bez znaczenia pozostaje również regulacja dotycząca jawności orzekania. Zgodnie z art. 67e ust. 2 Projektu Ustawy: *Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis*

¹⁰ Zob.: Certyfikacja zamiast blokowania – to odpowiedź na zmianę prawa, dostęp: <https://cyfrowa-gospodarka.gazetaprawna.pl/biznes/9506680.certyfikacja-zamiast-blokowania-to-odpowiedz-na-zmiane-prawa.html> (data dostępu: 02.12.2025 r.).

¹¹ Dz. U. z 2024 r. poz. 572 ze zm.; dalej: „k.p.a.”.

¹² Por. szerzej: A. Błaś, *Dylematy administracji publicznej w państwie prawa* [w:] *Prawo do dobrej administracji*, red. Z. Niewiadomski, Z. Cieślak, Warszawa 2003, s. 44-46; S. Wronkowska, *O stanowieniu i ogłaszaniu prawa oraz o kulturze prawnej*, Państwo i Prawo 4/2007, s. 3; S. Wronkowska, *Charakter prawny klauzuli demokratycznego państwa prawnego (art. 2 Konstytucji Rzeczypospolitej Polskiej)* [w:] *Zasada demokratycznego państwa prawnego*, red. S. Wronkowska, Warszawa 2006, s. 110.

wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych. Tym samym przedmiotowy przepis z art. 67e ust. 2 Projektu Ustawy wprowadza mechanizm doręczania stroną jedynie częściowego uzasadnienia, pod pretekstem anonimizacji informacji niejawnych. Jest to rozwiązanie niewspółmierne do standardu konstytucyjnego, zgodnie z którym wyrok sądu powinien być ogłaszany publicznie, a uzasadnienie jest jego integralną częścią. Konstytucja RP w art. 45 ust. 2 dopuszcza jedynie wyłączenie jawności rozprawy, ale nie uzasadnienia, co oznacza, że Projekt Ustawy tworzy regulację sprzeczną z zasadą jawności i dostępności wymiaru sprawiedliwości.

9. Kolejny problem ujawnia art. 67g ust. 2 Projektu Ustawy, który przewiduje możliwość formułowania przez ministra poleceń o skutku generalnym, kierowanych do nieokreślonego kręgu podmiotów. W świetle tego przepisu: *Polecenie zabezpieczające dotyczy nieokreślonej liczby podmiotów kluczowych lub podmiotów ważnych oraz podmiotów finansowych, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554*. Polecenia te nie mają postaci rozporządzenia, a mimo to nakładają powszechnie obowiązujące obowiązki. W ten sposób ustawodawca wykreował nową kategorię aktu *quasi*-normatywnego, która nie ma umocowania w art. 87 ust. 1 Konstytucji RP. Oznacza to naruszenie fundamentów systemu źródeł prawa, co może prowadzić do erozji zasady legalizmu i przejrzystości prawa.
10. Warto także zwrócić uwagę na budzący istotne wątpliwości projektowany przepis z art. 53e Projektu Ustawy: *1. Realizując uprawnienie, o którym mowa w art. 53 ust. 9, organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję, która zawiera:*
- 1) dane podmiotu kluczowego lub kierownika podmiotu kluczowego;*
 - 2) rodzaj stwierdzonych uchybień lub naruszeń dokonanych przez podmiot kluczowy lub kierownika podmiotu kluczowego;*
 - 3) podjęte dotychczas środki nadzorcze nad podmiotem kluczowym;*
 - 4) podstawę prawną i rodzaj środka określonego w art. 53 ust. 9;*
 - 5) termin stosowania tego środka;*
 - 6) uzasadnienie.*
- 2. Termin stosowania środków, o których mowa w art. 53 ust. 9, określa się przy uwzględnieniu kryteriów, o których mowa w art. 53 ust. 12. Środek nie może być stosowany dłużej niż 14 dni od daty doręczenia decyzji o jego zastosowaniu.*
- 3. W zależności od zastosowanego środka, jeżeli podmiot kluczowy usunął uchybienia lub zaprzestał naruszania przepisów ustawy przed terminem określonym w decyzji, uchyla się decyzję o zastosowaniu tego środka.*

4. W przypadku powzięcia informacji, w szczególności na skutek stosowania innych środków nadzorczych, określonych w art. 53 ust. 1, 4 i 5, że podmiot kluczowy nie usunął wcześniej stwierdzonych uchybień lub w dalszym ciągu narusza przepisy ustawy lub w przypadku gdy podmiot kluczowy nie wykazał w terminie, na jaki został zastosowany środek, że usunął uchybień lub zaprzestał naruszania przepisów ustawy, organ właściwy do spraw cyberbezpieczeństwa ponownie wydaje decyzję o zastosowaniu środka określonego w art. 53 ust. 9 na kolejny okres, nie dłuższy niż 14 dni. Przepis ten stosuje się do czasu usunięcia uchybień lub zaprzestania naruszeń przez podmiot kluczowy. W stosunku do ponownej decyzji nie stosuje się art. 53 ust. 13–16.

5. Organ właściwy do spraw cyberbezpieczeństwa z urzędu lub na wniosek podmiotu kluczowego uchyla decyzję, o której mowa w ust. 1, po usunięciu uchybień lub zaprzestaniu naruszeń przez podmiot kluczowy.

6. Podmiot kluczowy może złożyć wniosek, o którym mowa w ust. 5, po usunięciu uchybień lub zaprzestaniu naruszeń, przedstawiając dowody potwierdzające zastosowanie się odpowiednio do nakazu, o którym mowa w art. 53 ust. 5 pkt 1, lub postanowień decyzji, o której mowa w art. 53 ust. 5 pkt 2–8.

7. Wniosek, o którym mowa w ust. 5, organ właściwy do spraw cyberbezpieczeństwa rozpatruje niezwłocznie, nie później niż w terminie 7 dni od dnia jego otrzymania.

8. Czynności, o których mowa w ust. 3 i 5, organ dokonuje w formie decyzji.

9. Decyzja, o której mowa w ust. 1, jest wykonalna z dniem jej doręczenia podmiotowi kluczowemu. Decyzje, o których mowa w ust. 3, 4 i 5, są natychmiast wykonalne.

10. Postępowanie w sprawie stosowania i uchylania środków, o których mowa w art. 53 ust. 9, jest jednoinstancyjne. Na decyzje, o których mowa w ust. 1 i 3–5, podmiot kluczowy może wnieść skargę do sądu administracyjnego.

11. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o zastosowaniu wobec podmiotu kluczowego lub kierownika podmiotu kluczowego środków, o których mowa w art. 53 ust.

9. Informacja zawiera:

- 1) dane podmiotu kluczowego lub imię i nazwisko kierownika tego podmiotu kluczowego;
- 2) podstawę prawną i rodzaj zastosowanego środka, o którym mowa w art. 53 ust. 9;
- 3) wskazanie daty początkowej i końcowej okresu na jaki zastosowano środek;
- 4) wskazanie, czy wobec podmiotu kluczowego lub kierownika podmiotu kluczowego ponownie zastosowano środek, a jeśli tak, to wskazanie nowej daty końcowej stosowania tego środka.

12. Publikacja, o której mowa w ust. 11, nie obejmuje tajemnicy przedsiębiorstwa, jak również innych informacji podlegających ochronie na podstawie odrębnych przepisów.

13. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o uchyleniu decyzji, o której mowa w ust. 1.

14. Podmiot kluczowy, w okresie stosowania wobec niego środka, o którym mowa w art. 53 ust. 9, nie może wykonywać działalności, której dotyczy ten środek.

15. W okresie stosowania środka, o którym mowa w art. 53 ust. 9, podmiot kluczowy ma obowiązek niezwłocznie podjąć działania zmierzające jedynie do usunięcia uchybień bądź zaprzestania naruszeń. W tym celu w szczególności może składać oświadczenia woli i wiedzy, podejmować czynności procesowe w postępowaniach, przedsięwzierać czynności faktyczne, jeżeli nie stoją one w sprzeczności z celem stosowanego środka lub nie zmierzają do jego obejścia.

16. W zakresie nieuregulowanym, a dotyczącym zawieszania, ograniczania i wznawiania koncesji, zezwolenia na prowadzenie działalności gospodarczej lub wstrzymania prowadzenia działalności gospodarczej zastosowanie mają przepisy odrębne.

11. W przepisie z art. 53e Projektu Ustawy określono elementy obligatoryjne decyzji nakładającej środek (identyfikacja podmiotu/kierownika, opis uchybień lub naruszeń, dotychczasowe środki nadzorcze, podstawa i rodzaj środka z art. 53 ust. 9 Projektu Ustawy, termin jego stosowania oraz uzasadnienie). Decyzja jest wykonalna z chwilą doręczenia. W okresie stosowania środka podmiot nie może wykonywać działalności, której środek dotyczy. Jednocześnie ma obowiązek niezwłocznie podjąć wyłącznie działania zmierzające do usunięcia uchybień lub zaprzestania naruszeń (w tym składać oświadczenia, podejmować czynności procesowe i faktyczne), o ile nie są sprzeczne z celem środka ani nie zmierzają do jego obejścia. Postępowanie w sprawie stosowania i uchylania środków z art. 53 ust. 9 ww. regulacji jest jednoinstancyjne. Na decyzje o zastosowaniu środka oraz o jego uchyleniu/utrzymaniu (ust. 1 i 3–5) przysługuje skarga do sądu administracyjnego.
12. W rezultacie całościowa ocena mechanizmu art. 67b i nast. Projektu Ustawy prowadzi do jednoznacznego wniosku, że regulacje te nie spełniają konstytucyjnego testu proporcjonalności, naruszają zasadę rzetelności procesu prawotwórczego oraz prowadzą do ingerencji w istotę prawa własności i wolności działalności gospodarczej. Wymogi te nie są spełnione ani na poziomie formalnym, ani materialnym, a dodatkowo projekt pomija standardy wynikające z prawa Unii Europejskiej, prowadząc do nadregulacji, która jest nie tylko niezasadna, ale i sprzeczna z zasadą demokratycznego państwa prawnego. Taki sposób stanowienia prawa osłabia zaufanie do państwa, destabilizuje otoczenie prawne przedsiębiorców i tworzy mechanizmy ingerencji, które nie znajdują oparcia ani w Konstytucji, ani w unijnym porządku prawnym.

13. W konsekwencji niniejsza opinia na zasadzie *amicus curiae* zostanie poświęcona systematycznemu wykazaniu wszystkich powyższych wątków oraz ocenie ich w świetle obowiązujących przepisów prawa Unii Europejskiej i krajowego, w tym w kontekście proporcjonalności środków, legalności ingerencji w prawa własności, respektowania swobód gospodarczych oraz standardów proceduralnych przewidzianych w Konstytucji RP i prawie unijnym. Rezultatem przedstawionej analizy będzie wyraźne określenie zakresu niezgodności projektowanych przepisów ujętych w treści Projektu Ustawy z prawem Unii Europejskiej i Konstytucją RP, jak również wskazanie ryzyk wynikających z ich przyjęcia.

III.2. *Gold-plating* i Dyrektywa NIS2 jako dyrektywa minimalnej harmonizacji.

14. W pierwszej kolejności należy na potrzeby niniejszej opinii na zasadzie *amicus curiae* doprecyzować pojęcie *gold-platingu*, które, pomimo swojej częstej obecności zarówno w doktrynie, jak i w praktyce legislacyjnej państw członkowskich, nie doczekało się jednolitej i powszechnie akceptowanej definicji normatywnej¹³. Termin ten, choć intuicyjnie rozpoznawalny, funkcjonuje raczej jako konstrukcja opisowa, wykorzystywana do odzwierciedlenia sytuacji, w których prawodawca krajowy, realizując obowiązek transpozycji dyrektywy unijnej, wykracza poza minimalny zakres wynikający z jej literalnego brzmienia bądź celu regulacyjnego¹⁴, co skutkuje nałożeniem na adresatów dodatkowych, niewymaganych przez prawo unijne obowiązków.
15. W ujęciu przyjmowanym przez instytucje Unii Europejskiej, *gold-plating* obejmuje zatem w szczególności takie przypadki, w których prawodawca krajowy wprowadza do legislacji krajowej rozwiązania materialne lub proceduralne niemające oparcia w dyrektywie unijnej¹⁵, rezygnuje z możliwości zastosowania przewidzianych w niej wyjątków lub derogacji, bądź decyduje się na ustanowienie mechanizmów sankcyjnych o surowszym charakterze niż te, które są konieczne do osiągnięcia celu tej dyrektywy¹⁶. Przyjęcie takiej

¹³ Zob. np.: K. Kaczor, *Gold-plating - problem nadtranspozycji dyrektyw unijnych do krajowego porządku prawnego*, *Folia Iuridica Universitatis Wratislaviensis* 2022, nr 11 (1), s. 76-98.

¹⁴ Por. np.: K. Atthoff, M. Wallgren, *Clarifying Gold-Plating* Karin Atthoff and Mia Wallgren - Better Implementation of EU Legislation, s. 25-26; R. Král, *National Public Interest Grounds Justifying Gold-Plating of EU Law*, w: L. Tichý, M. Potacs (red.), *Public Interest in Law*, Cambridge: Cambridge University Press 2021, s. 109-110; „Differences between harmonized company law and domestic rules: the phenomena of ‘gold plating’ and ‘circumvention’ of EU law”, *ADVANT Nctm*, 3.10.2022 r., dostępny: <https://www.advant-nctm.com/en/news/differences-between-harmonized-company-law-and-domestic-rules-the-phenomena-of-gold-plating-and-circumvention-of-eu-law> (data dostępu: 02.12.2025 r.).

¹⁵ K. Atthoff, M. Wallgren, *Clarifying Gold-Plating* Karin Atthoff and Mia Wallgren – Better Implementation of EU Legislation, s. 28; zob. także: L. Squintani, *Gold-Plating: A Misleading Overarching Concept*, w: L. Squintani (red.), *Beyond Minimum Harmonisation: Gold-Plating and Green-Plating of European Environmental Law*, Cambridge: Cambridge University Press 2019, s. 26-27.

¹⁶ „Differences between harmonized company law and domestic rules: the phenomena of ‘gold plating’ and ‘circumvention’ of EU law”, *ADVANT Nctm*, 3.10.2022 r., dostępny: <https://www.advant-nctm.com/en/news/differences-between-harmonized-company-law-and-domestic-rules-the-phenomena-of-gold-plating-and-circumvention-of-eu-law> (data dostępu: 02.12.2025 r.).

perspektywy pozwala odróżnić działania stanowiące uzasadnioną adaptację struktury prawa krajowego od aktywności prowadzących do nadmiernego obciążania podmiotów regulacji, a w konsekwencji - do powstania stanu nadregulacji¹⁷.

16. Właściwe uchwycenie istoty *gold-platingu* wymaga osadzenia go w szerszym kontekście normatywnym charakterystycznym dla dyrektyw jako instrumentów prawa wtórnego Unii Europejskiej. W tym kontekście zauważyć należy, że dyrektywy unijne nie wywołują skutku bezpośredniego w krajowym porządku prawnym, co oznacza że ich normatywna treść wymaga implementacji poprzez działania legislacyjne państwa członkowskiego.
17. W powyższym kontekście dostrzec należy, że transpozycja, będąca podstawowym elementem tego procesu, polega na przeniesieniu do krajowego systemu prawnego minimalnych wymogów wynikających z dyrektywy, z zachowaniem swobody co do formy i środków służących realizacji założonego celu. Implementacja ma jednak charakter szerszy, obejmuje bowiem nie tylko samo przeniesienie treści dyrektywy unijnej, lecz również zapewnienie jej skutecznego stosowania przez organy administracji i sądy krajowe¹⁸. W tym właśnie obszarze pojawia się przestrzeń, w której *gold-plating* może się ujawnić - jest on bowiem nierozzerwalnie związany z działaniami podejmowanymi przy i w następstwie implementacji, w szczególności z wyborem legislacyjnym dotyczącym zakresu, intensywności i formy regulacji przyjmowanej na poziomie krajowym.
18. Szczególnego znaczenia nabiera to w odniesieniu do Dyrektywy NIS2, która - zgodnie z art. 5 Dyrektywy NIS2¹⁹ - stanowi klasyczny przykład aktu harmonizacji minimalnej²⁰. Oznacza to, że prawodawca unijny zdecydował się na wyznaczenie jedynie minimalnego poziomu wymagań, których realizacja jest obligatoryjna dla państw członkowskich, pozostawiając im szeroki margines swobody w zakresie ewentualnego zaostrzenia lub doprecyzowania przyjmowanych rozwiązań. Tym samym Dyrektywa NIS2 nie tylko dopuszcza, lecz wręcz zakłada możliwość wprowadzania przez państwa członkowskie regulacji bardziej rygorystycznych, o ile mieszczą się one w granicach wyznaczonych przez prawo Unii Europejskiej oraz pozostają spójne z celami Dyrektywy NIS2.
19. W rezultacie prawodawca krajowy może, w sposób niesprzeczny z dyrektywą unijną, zarówno doprecyzować kryteria identyfikacji podmiotów uznawanych za kluczowe lub ważne w rozumieniu reżimu wprowadzonego w treści Dyrektywy NIS2, jak i nałożyć na nie dodatkowe obowiązki o charakterze technicznym lub organizacyjnym, które uzna za

¹⁷ Zob. szerzej: T. Siemiątkowski, Szkodliwa nadregulacja w sprawie cyberbezpieczeństwa, dostęp: <https://www.rp.pl/opinie-prawne/art41473571-prof-tomasz-siemiatkowski-szkodliwa-nadregulacja-w-sprawie-cyberbezpieczenstwa> (data dostępu: 02.12.2025 r.).

¹⁸ Por.: J. Maśnicki, Metody transpozycji dyrektyw, EPS 2017, nr 8, s. 4-5.

¹⁹ Artykuł 5 (*Harmonizacja minimalna*): *Niniejsza dyrektywa nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązkami państw członkowskich, ustanowionymi w prawie Unii.*

²⁰ Por. szerzej: R.A. Tokarczyk, Problemy harmonizacji polskiej kultury prawnej z kulturą prawną Unii Europejskiej, St.Europ. 2004, nr 3, s. 71.

niezbędne z punktu widzenia ochrony krajowych interesów bezpieczeństwa. Może również zdecydować o wprowadzeniu bardziej szczegółowych mechanizmów nadzorczych i sankcyjnych, o ile działanie to będzie mieścić się w ramach zasad prawa unijnego oraz prawa krajowego, w tym Konstytucji RP.

20. Swoboda prawodawcy krajowego nie ma jednak charakteru absolutnego, ponieważ granice jego aktywności wyznaczane są zarówno przez normy prawa pierwotnego Unii Europejskiej (w szczególności zasady proporcjonalności, zasady swobodnego przepływu towarów i usług oraz swobody przedsiębiorczości), jak i przez krajowe zasady konstytucyjne, ze szczególnym uwzględnieniem zasady proporcjonalności.
21. Rozważania dotyczące dopuszczalnego zakresu uzupełniania regulacji ujętej w treści Dyrektywy NIS2 na poziomie krajowym muszą prowadzić do stwierdzenia, że jakiegokolwiek działanie prawodawcy wykraczające poza minimum wynikające z dyrektywy unijnej musi spełniać określone kryteria, warunkujące jego legalność i zgodność z porządkiem unijnym oraz konstytucyjnym.
22. Po pierwsze, regulacja taka musi pozostawać zgodna z prawem wyższego rzędu, co oznacza konieczność respektowania zarówno norm Konstytucji RP, jak i traktatowych zasad prawa Unii Europejskiej.
23. Po drugie, wszelkie wprowadzone środki muszą odpowiadać zasadzie proporcjonalności, co oznacza, że ich intensywność i zakres nie mogą wykraczać poza to, co jest konieczne do osiągnięcia zakładanego celu regulacyjnego.
24. Po trzecie, zgodnie z zasadą subsydiarności, interwencja krajowa może zostać podjęta jedynie wówczas, gdy cel regulacji nie może zostać osiągnięty w sposób wystarczający na poziomie unijnym lub gdy interwencja krajowa jest lepiej dostosowana do specyfiki danego obszaru.
25. Po czwarte, prawodawca krajowy musi działać w sposób transparentny, co wiąże się z koniecznością przeprowadzenia rzetelnej analizy skutków regulacji oraz przedstawienia przekonującego uzasadnienia dla każdego rozwiązania wykraczającego poza minimum unijne.
26. Po piąte wreszcie, regulacje krajowe muszą pozostawać w pełni kompatybilne z prawem Unii Europejskiej i nie mogą prowadzić do powstania barier utrudniających funkcjonowanie rynku wewnętrznego ani też do dyskryminacji podmiotów zagranicznych względem podmiotów krajowych.
27. Dopiero łączne spełnienie powyższych warunków pozwala uznać, że zastosowany przez prawodawcę krajowego *gold-plating* ma charakter dopuszczalny i mieści się w ramach wyznaczonych przez prawodawcę unijnego. W przeciwnym wypadku działania takie mogą prowadzić do powstania regulacji nadmiernie restrykcyjnych, nieuzasadnionych lub wręcz

sprzecznych z prawem unijnym²¹, co z kolei generuje ryzyko sporów prawnych oraz odpowiedzialności państwa za naruszenie prawa Unii Europejskiej.

III.3. Ocena sposobu implementacji Dyrektywy NIS2 przez prawodawcę krajowego z perspektywy zgodności z przepisami prawa Unii Europejskiej.

28. Wskazać także należy, że Projekt Ustawy, choć deklaruje wprost, że jego celem jest wdrożenie Dyrektywy NIS2, już w pierwszych swoich założeniach uwidacznia konflikt pomiędzy zakładaną funkcją implementacyjną a rzeczywistą treścią przyjętych rozwiązań. Wskazane w przypisach Projektu Ustawy odwołania do Rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej²² oraz do zestawu zaleceń 5G Toolbox tworzą obraz regulacji, która w praktyce nie ogranicza się do przeniesienia do polskiego porządku prawnego minimum unijnego wynikającego z Dyrektywy NIS2, lecz przekształca się w akt o znacznie szerszym zasięgu, obejmujący komponenty prawnie niewiążące, a jednocześnie narzucający podmiotom obowiązki dalece wykraczające poza to, czego wymaga prawo unijne.
29. W powyższym kontekście raz jeszcze należy podkreślić, iż Dyrektywa NIS2 stanowi akt harmonizacji minimalnej, co oznacza, że państwa członkowskie mogą wykraczać poza jej standardy, o ile robią to w sposób zgodny z prawem wyższego rzędu, proporcjonalny i oparty na dowodach. Tymczasem Projekt Ustawy, zamiast respektować tę architekturę kompetencyjną, przekształca 5G Toolbox - instrument o charakterze *soft law*, niewiążący na gruncie art. 288 TFUE - w faktyczne źródło kompetencji prawotwórczej. Przekształca rekomendacje techniczne w normy prawne o skutku bezpośrednio ograniczającym prawa podmiotów gospodarczych.
30. Tego rodzaju zabieg narusza podstawową zasadę wykładni i stosowania prawa unijnego, zgodnie z którą *soft law* może ukierunkowywać interpretację przepisów wiążących, lecz nie może tworzyć obowiązków²³, których dyrektywa nie przewiduje, a tym bardziej nie

²¹ Zob. np.: M. Jabłoński, The Danger of So-Called Regulatory 'Gold-Plating' in Transposition of EU Law - Lessons from Poland, „Studia Iuridica” 2017, vol. 71, s. 76; por. także np.: krytyczne stanowiska instytucji i organów unijnych wobec gold-platingu, m.in.: rezolucję Parlamentu Europejskiego w sprawie wdrażania, konsekwencji i wpływu obowiązującego prawodawstwa dotyczącego rynku wewnętrznego (2004/2224 INI); komunikat Komisji dla Rady i Parlamentu Europejskiego z dnia 16 marca 2005 r.: Poprawa otoczenia regulacyjnego w dziedzinie wzrostu gospodarczego i zatrudnienia w Unii Europejskiej (SEC(2005) 175); opinię Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Realizacja wspólnotowego programu lizbońskiego: strategia w zakresie uproszczenia otoczenia regulacyjnego (2006/C 309/04).

²² Dz. U. UE. L. z 2024 r. poz. 1366 ze zm.

²³ Zob. np.: A. Szumański, Normy *soft law* ich rodzaje we współczesnym międzynarodowym prawie handlowym, PPH 2025, nr 6, s. 16-25.

może stanowić uzasadnienia ustawowego rozszerzenia zakresu władztwa organów administracji państwowej.

31. Właśnie w tej perspektywie - z uwzględnieniem hierarchii źródeł prawa oraz zasady pierwszeństwa i skuteczności prawa UE - należy ocenić regulacje projektu dotyczące wyznaczania dostawców wysokiego ryzyka, a więc dostawców wysokiego ryzyka. Konstrukcja ta, osadzona nominalnie w logice bezpieczeństwa narodowego, jest w istocie odwzorowaniem mechanizmów postulowanych w 5G Toolbox, lecz zastosowanym w formie o wiele szerszej niż przewidywały to założenia unijne. Zamiast objąć takim reżimem sektor telekomunikacyjny i infrastrukturę 5G, co odpowiadałoby celowi, dla którego 5G Toolbox w ogóle został opracowany, Projekt Ustawy rozszerza go na wszystkie sektory kluczowe i ważne wymienione w Dyrektywie NIS2: na energetykę, zdrowie, transport, gospodarkę wodną, sektor chemiczny, usługi cyfrowe, zarządzanie infrastrukturą cyfrową, sektor kosmiczny, żywność, naukę oraz sektor publiczny²⁴.
32. Tak szeroki zakres oddziaływania w sposób oczywisty wykracza poza to, co Dyrektywa NIS2 dopuszcza, a jednocześnie narusza jej strukturę logiczną. Dyrektywa NIS2 wymaga, aby wszelkie działania krajowe - zarówno te wynikające wprost z dyrektywy, jak i te, które państwo członkowskie podejmuje w ramach przysługującego mu marginesu swobody - były oparte na rzetelnych, sektorowych analizach ryzyka. To jest fundament całej dyrektywy, jednoznacznie potwierdzony w licznych motywach jej preambuły, w szczególności w motywie 91²⁵. Państwo członkowskie nie może zatem wprowadzać rozwiązań uderzających w dostęp do rynku ani ograniczających korzystanie z określonych technologii, jeżeli nie wykaże konkretnych, mierzalnych i empirycznie stwierdzonych podstaw takiej interwencji.
33. Projekt Ustawy nie spełnia tego kryterium. Brakuje uzasadnienia opartego na dowodach, brak jest sektorowych ocen ryzyka, nie wskazano skali ani natury zagrożeń, które miałyby uzasadniać tak szeroką ingerencję. W miejsce ugruntowanej empirii pojawia się jedynie odwołanie do ogólnych możliwości zagrożeń związanych z wykorzystaniem technologii

²⁴ Por. np.: <https://www.pwc.pl/pl/uslugi/nis2-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html> (data dostępu: 02.12.2025 r.).

²⁵ Zgodnie z motywem 91 Dyrektywy NIS2: *W świetle specyfiki danego sektora w skoordynowanych oszacowaniach ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw należy uwzględnić zarówno czynniki techniczne, jak i – w stosownych przypadkach – pozatechniczne, w tym te określone w zaleceniu (UE) 2019/534, w unijnym skoordynowanym oszacowaniu ryzyka dotyczącym cyberbezpieczeństwa sieci 5G oraz w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G uzgodnionym przez Grupę Współpracy. Aby zidentyfikować łańcuchy dostaw, które należy poddać skoordynowanemu oszacowaniu ryzyka dla bezpieczeństwa, należy wziąć pod uwagę następujące kryteria: (i) zakres, w jakim podmioty kluczowe i ważne wykorzystują konkretne krytyczne usługi ICT, systemy ICT lub produkty ICT i są od nich zależne; (ii) znaczenie konkretnych krytycznych usług ICT, systemów ICT lub produktów ICT dla wykonywania krytycznych lub wrażliwych funkcji, w tym przetwarzania danych osobowych; (iii) dostępność alternatywnych usług ICT, systemów ICT lub produktów ICT; (iv) odporność całego łańcucha dostaw usług ICT, systemów ICT lub produktów ICT, w ciągu ich cyklu życia, na zdarzenia powodujące zakłócenia; (v) w przypadku pojawiających się usług ICT, systemów ICT lub produktów ICT – ich potencjalne przyszłe znaczenie dla działalności podmiotów. Ponadto szczególny nacisk należy położyć na usługi ICT, systemy ICT lub produkty ICT podlegające specjalnym wymogom pochodzącym z państw trzecich.*

pochoǳących spoza Unii Europejskiej. Tak szeroki i niezróznicowany katalog podmiotów uznanych za potencjalnie zagroonych prowadzi do naruszenia zasady proporcjonalnoŹci - jednej z fundamentalnych zasad prawa unijnego.

34. W powyższym kontekŹcie podkreŹlić naleŹy, Źe jednym z fundamentalnych wymogów wynikających z porządku unijnego i porządku krajowego jest to, by wszystkie rozwiązania normatywne były proporcjonalne. Oznacza to, Źe kaŹde rozwiązanie legislacyjne powinno być niejako „szyte na miarę”, a zatem powinny być idealnie dopasowane do celu regulacyjnego, którego urzeczywistnieniu te rozwiązania słuŹą²⁶.
35. Zasadą obowiąŹzującą tak w porządku prawa Unii Europejskiej, jak i w prawie krajowym nakierowaną na realizację okreŹlonego powyŹej celu jest zasada proporcjonalnoŹci. Ze względu na istotnoŹć tej zasady dla oceny Projektu Ustawy, warto przedstawić tę zasadę - w pierwszej kolejnoŹci w kontekŹcie jej funkcjonowania w ramach systemu prawa Unii Europejskiej, a następnie - w odniesieniu do polskiego porządku konstytucyjnego.
36. Zasada proporcjonalnoŹci uznawana za jedną z zasad ogólnych, podstawowych prawa Unii Europejskiej²⁷, jak równieŹ - zasadę o walorze konstytucyjnym²⁸. Stanowi ona jedną z najwaŹniejszych zasad, na których oparty jest porządek prawny Unii Europejskiej²⁹; gdzie na gruncie prawa Unii Europejskiej wynika ona z art. 5 ust. 4 Traktatu o Unii Europejskiej³⁰, zgodnie z którym: *zakres i forma działania Unii nie wykraczają poza to, co jest konieczne do osiągnięcia celów Traktatów*³¹.
37. Podstawową funkcją realizowaną przez zasadę proporcjonalnoŹci jest ograniczenie – nieuzasadnionych, w okreŹlonej sytuacji, koniecznoŹcią ochrony interesu publicznego – działań organów władzy publicznej ingerujących w sferę chronionych wolnoŹci i praw podmiotowych. Realizacja tego celu następuje poprzez okreŹlenie przesłanek, których wystąpienie uzasadnia wprowadzenie takiego ograniczenia.

²⁶ M. Źliwa-Wajda, P. Wajda, *Konsultacje projektów rekomendacji prowadzone przez Komisję Nadzoru Finansowego – aspekty prawnounijne*, WiadomoŹci Ubezpieczeniowe 2/2023, s. 3-26.

²⁷ Por. np.: D. Sobczyński, *Zasada proporcjonalnoŹci w europejskim prawie wspólnotowym*, „Głosa Przegląd. Prawa Gospodarczego” 2003, nr 3, s. 7.

²⁸ Por. np.: P. Tuleja [w:] P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radziejewicz, P. Tuleja, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, wyd. II, LEX/el. 2021, art. 31.

²⁹ Tym samym stanowi zasadę, która bepoŹrednio obowiąŹzuje we wszystkich państwach członkowskich i to niezaleŹnie od jej bepoŹredniego wprowadzenia do porządku prawnego danego państwa; por. szerzej: J. Barcz, *Zasada pierwszeństwa prawa wspólnotowego w Źwietle postanowień Konstytucji RP z 1997 r.*, „Kwartalnik Prawa Publicznego” 2004, nr 2, s. 21-42; por. takŹe: K. Wójtowicz, *BepoŹredni skutek przepisów prawa wspólnotowego w porządku prawnym RP*, „Kwartalnik Prawa Publicznego” 2004, nr 1, s. 43-70; por. takŹe: wyrok TSUE z dnia 5 lutego 1963 r. w sprawie C- 26/62 NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, Zb. Orz. 1963, s. 00003.

³⁰ Dz. U. z 2004 r. Nr 90, poz. 864/30 ze zm.

³¹ Por.: wyrok TSUE z dnia 10 stycznia 2006 r. w sprawie C-344/04 The Queen on the application of: International Air Transport Association and European Low Fares Airline Association vs Department for Transport, [Zb. Orz. 2006, s. I-00403](#).

38. Zasada ta stanowi zasadniczą wytyczną odnośnie do wykonywania kompetencji przyznanych w traktatach instytucjom Unii Europejskiej, jak i – z uwagi na recypowanie tej zasady do krajowych porządków normatywnych – kompetencji przyznanych instytucjom krajowym i równocześnie stanowi zasadnicze kryterium weryfikacji prawidłowości realizacji tych kompetencji. Zasada proporcjonalności wyznacza wytyczne dla władzy wykonawczej w obrębie Unii Europejskiej (tak na szczeblu UE, jak i na szczeblu krajowym) i chroni tym samym państwa członkowskie UE przed ingerencją UE w ich zakres władzy, jak również jednostki przed nadmierną i nieuzasadnioną³² okolicznościami danego przypadku ingerencją uprawnionych organów władzy wykonawczej w ich działalność.
39. Zasada proporcjonalności wymaga, aby środki służące wykonaniu prawa UE i krajowego były ściśle dostosowane do okoliczności sprawy; organy nie mogą stosować nadmiernie dolegliwych rozwiązań ani nakładać nieuzasadnionych obciążeń. Zasada ta wyznacza standard zarówno dla regulacji, jak i działań organów, ma charakter jurydyczny i może być powoływana przed sądami jako wzorzec kontroli legalności. Zastosowany środek powinien możliwie skutecznie prowadzić do osiągnięcia celu regulacyjnego; środki zbyt restrykcyjne, które nie zapewniają tego rezultatu, naruszają proporcjonalność. Gdy dostępnych jest kilka rozwiązań, organ musi wybrać najprostsze, najtańsze i najmniej dolegliwe. Niedogodności dla państwa lub jednostek muszą pozostawać w rozsądnej relacji do celu; instrument nie może powodować, że koszty społeczne i gospodarcze istotnie przewyższają wartość osiąganego celu.
40. W świetle stanowiska Trybunału Sprawiedliwości Unii Europejskiej odnośnie do praktycznego ujmowania tej zasady podjęty środek musi zawsze spełniać tzw. test proporcjonalności; tj. być nie tylko konieczny dla osiągnięcia celu, ale również odpowiedni (adekwatny) i proporcjonalny *sensu stricto* (współmierny). Wskazany test stanowi obiektywny standard oceny legalności wprowadzonych ograniczeń wolności i praw³³.
41. Na test proporcjonalności składają się trzy zasadnicze wymogi: (i) wymóg przydatności (odpowiedniości) - który sprowadza się do dokonania oceny, czy wykorzystanie danego środka prawnego ingerencji jest zdolne do doprowadzenia do osiągnięcia zamierzonego przez prawodawcę celu; (ii) wymóg konieczności (niezbędności) - który sprowadza się do stosowania reguły najmniejszej ingerencji, tzn. do osiągnięcia danego celu należy wybrać

³² Por. np.: wyrok TSUE z dnia 14 maja 1974 r., w sprawie C-4/73 J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities, *Zb. Orz.* 1974, s. 00491; wyrok TSUE w sprawie C-11/70 Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel; wyrok TSUE z dnia 13 grudnia 1979 r., w sprawie C-44/79 Liselotte Hauer przeciwko Land Rheinland-Pfalz, *Zb. Orz.* 1979, s. 03727; wyrok TSUE z dnia 20 września 2003 r. w sprawie C-320/03 Komisja Europejska przeciwko Republice Austrii, *Zb. Orz.* 2005, s. I-09871; wyrok TSUE z dnia 21 grudnia 2011 r. w sprawie C-28/09 Komisja Europejska v Austria Komisja Europejska przeciwko Republice Austrii, *Zb. Orz.* 2011, s. I-13525.

³³ Por. np.: wyrok TK z dnia 27 stycznia 1999 r., K 1/98, *Legalis*; wyrok TK z dnia 20 listopada 2002 r., K 41/02, *OTK* 1999, nr 1, poz. 3; por. także: wyrok TK z 5.04.2011 r., P 26/09, *OTK-A* 2011, nr 3, poz. 18; wyrok TK z 13.03.2007 r., K 8/07, *OTK-A* 2007, nr 3, poz. 26; wyrok TK z 23.04.2008 r., SK 16/07, *OTK-A* 2008, nr 3, poz. 45.

ten z środków, który w najmniejszym stopniu wkracza w prawa i wolności jednostki; oraz (iii) wymóg zachowania proporcjonalności wprowadzonego ograniczenia do zamierzonego celu (zasada proporcjonalności *sensu stricto*) - który sprowadza się do zbilansowania czy dobro (prawo, wolność) chronione w wyniku ingerencji prawodawcy jest dobrem na tyle ważnym i istotnym, że jego ochrona uzasadnia konieczność ograniczenia innych praw czy wolności.

42. Zasada proporcjonalności jest swoistym mechanizmem „ważenia” wartości, konfrontowania zasad, praw i wolności, poszukiwania idealnego punktu równowagi³⁴. Wymaga ona, by środki i działania podejmowane zarówno przez instytucje unijne, państwa członkowskie oraz uprawnione podmioty administrujące były odpowiednie i niezbędne do osiągnięcia celu, któremu służą³⁵. Zasada proporcjonalności wymaga od prawodawcy wprowadzającego ograniczenie w zakresie obowiązywania prawa podmiotowego równoległego i kumulatywnego spełnienia kilku warunków³⁶. Po pierwsze, istotnym motywem wprowadzenia takiego ograniczenia musi być cel, ze względu, na którego realizację to ograniczenie ma nastąpić. Prawodawca, decydując się na ograniczenie danego prawa, działać ma zawsze w imię realizacji dobra publicznego, skonkretyzowanego w postaci określonego celu publicznego. Po drugie, ograniczenie to ma być środkiem mającym zapewnić realizację danego celu publicznego. Po trzecie, musi zostać spełniony wymóg przydatności środka, który dotyczy relacji występującej pomiędzy ograniczeniem prawa jako środkiem a celem, który ma być osiągnięty w wyniku zastosowania tego środka. Ograniczenie to ma być zabiegiem rzeczywiście przydatnym dla realizacji zamierzonego przez ustawodawcę celu. Po czwarte, ograniczenie to musi przyjąć postać najmniejszego potencjalnie możliwego ograniczenia, które jest jednocześnie ograniczeniem wystarczającym do osiągnięcia zamierzonego celu. Po piąte wreszcie, ustawodawca musi pamiętać, że nie wolno mu ograniczać konstytucyjnego prawa podmiotowego nawet wówczas, gdy ograniczenie jest środkiem przydatnym dla osiągnięcia danego celu, jeśli sam charakter celu takiego ograniczenia nie usprawiedliwia³⁷.

³⁴ Por. szerzej: M. Safjan, *Wyzwania dla państwa prawa*, Warszawa 2007, s. 79-80 i s. 155; por. także: wyrok TK z dnia 26 października 2005 r., K 31/04, OTK 2005, seria A, nr 9, poz. 103.

³⁵ Por. szerzej: T. Tridimas, *The Principles of Proportionality and Subsidiarity under the EU Constitution* [w:] *Reformowanie Unii Europejskiej. Wybrane problemy prawne okresu przemian*, E. Piontek (red.), Zakamycze 2005, s. 100.

³⁶ Por. szerzej: wyrok TK z dnia 16 lutego 1999 r., Sk. 11/98, OTK 1999, Nr 2, poz. 22.

³⁷ Por. szerzej: A. Walaszek-Pyziół, *Zasada proporcjonalności w orzecznictwie Trybunału Konstytucyjnego*, Przegląd Ustawodawstwa Gospodarczego 1995 nr 1, s. 15-16; D. Sobczyński, *Zasada proporcjonalności w europejskim prawie wspólnotowym*, „Glosa Przegląd. Prawa Gospodarczego” 2003, nr 3, s. 10-11. Wyrok Trybunału Konstytucyjnego z dnia 9 czerwca 1998 r., K. 28/97, OTK 1998, Nr 4, poz. 50; Por. także Wyrok SN z dnia 6 kwietnia 2001 r., III RN 87/00; OSNP 2001, poz. 704; M. Zdyb, J. Stelmasiak, J. Szreniawski, *Zasada proporcjonalności w świetle Konstytucji RP* [w:] *Podmioty administracji publicznej i prawne formy ich działania. Studia i materiały z Konferencji Naukowej Poświęconej Jubileuszowi 80-tych urodzin Profesora Eugeniusza Ochendowskiego*. Toruń, 15-16 listopada 2005, Toruń 2005, s. 471-481.

43. Zasada proporcjonalności znajduje zastosowanie tak do aktów prawnych wydawanych przez instytucje UE, jak i do aktów wydawanych na szczeblu państw członkowskich. Respektowanie zasady proporcjonalności pozwala na pogodzenie interesu UE z interesami państw członkowskich, co przekłada się na zapewnienie faktycznej możliwości funkcjonowania rynku wewnętrznego. Zasada ta pozwala bowiem wyeliminować z obrotu prawnego regulacje stojące w opozycji do swobód rynku wewnętrznego UE (co ma również istotne znaczenie w odniesieniu do oceny Projektu).
44. Zasada proporcjonalności stanowi istotne kryterium oceny legalności unijnych aktów prawnych i kierowanych do konkretnych adresatów aktów, oraz stanowi jeden z fundamentów dla uregulowania stosunków Unii Europejskiej z państwami członkowskimi (przez rozgraniczenie przysługujących im kompetencji, jak i przez sformułowanie kryteriów dla dokonywania oceny legalności konkretnego działania czy aktu prawnego)³⁸. Jest także kryterium pozwalającym na dokonanie oceny legalności, celowości, a także racjonalności poszczególnych regulacji należących do krajowego porządku normatywnego oraz konkretnych zachowań i działań podejmowanych przez uprawnione podmioty wchodzące w skład aparatu administracji publicznej.
45. Uwzględniając powyższe stwierdzić należy, że środki ograniczające działalność gospodarczą muszą pozostawać w relacji adekwatności i niezbędności³⁹ do celu, który mają osiągnąć⁴⁰. Projekt Ustawy nakłada jednak ograniczenia o charakterze całkowitym, obejmujące obowiązek wycofania sprzętu i usług ICT z infrastruktury bez jakiegokolwiek analizy sektorowej czy oceny, czy dany komponent faktycznie generuje zagrożenie. W efekcie uznanie dostawcy za dostawcę wysokiego ryzyka staje się decyzją o skutkach absolutnych, rozciągających się na całość działalności danego podmiotu, choć zagrożenie może dotyczyć jedynie wąskiej części jego produktów. To rażące naruszenie zasady proporcjonalności w jej wymiarze zarówno materialnym, jak i funkcjonalnym.
46. Równocześnie Projekt Ustawy ustanawia mechanizmy administracyjne o charakterze *quasi*-prewencyjnym, które nie mają oparcia w logice Dyrektywy NIS2. Ustawa przewiduje, że wszczęcie postępowania w sprawie uznania dostawcy za dostawcę

³⁸ Por. szerzej: G. Grabowska, *Podział kompetencji między Unią Europejską a jej państwami członkowskimi. „Kto ma jakie uprawnienia w UE?”* [w:] *Administracja pod wpływem prawa europejskiego. XIV Niemiecko-Polskie Kolokwium Prawników Administratywistów. Katowice 14-17 września 2005 roku. Referaty i głosy w dyskusji*, B. Dolnicki (red.), J. Jagoda (red.), Bydgoszcz-Katowice 2006, s. 51; D. Kugelman, *Wpływ prawa europejskiego na ustrój administracji państw członkowskich* [w:] *Administracja pod wpływem prawa europejskiego. XIV Niemiecko-Polskie Kolokwium Prawników Administratywistów. Katowice 14-17 września 2005 roku. Referaty i głosy w dyskusji*, B. Dolnicki (red.), J. Jagoda (red.), Bydgoszcz-Katowice 2006, s. 120-121.

³⁹ Tak też: K. Zaradkiewicz [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016, art. 21; zob. także: Wyrok TK z dnia 13 grudnia 2012 r.; sygnatura: P 12/11; OTK-A 2012/11/135; Wyrok NSA z dnia 4 grudnia 2014 r.; sygnatura: I OSK 1049/13; LEX nr 2008779; Wyrok NSA z dnia 21 marca 2013 r.; sygnatura: I OSK 1722/12; LEX nr 1436988.

⁴⁰ Tak też: K. Klecha, *Wolność działalności gospodarczej w Konstytucji RP*, Warszawa 2009, s. 220; S. Korus, *Ochrona zdrowia jako przejaw ważnego interesu publicznego w rozumieniu art. 22 Konstytucji RP w dobie epidemii choroby COVID-19*, Warszawa 2020, s. 143 i nast.

wysokiego ryzyka jest uzależnione od opinii Kolegium ds. Cyberbezpieczeństwa, które z kolei opiera się na analizach przeprowadzanych przez CSIRT-y. Tymczasem kryteria, jakie mają być podstawą takiej analizy, pozostają ogólne i niewystarczająco precyzyjne. Brak ich dookreślenia sprawia, że organy administracji państwowej uzyskują szerokie i niekontrolowalne uznanie, co w unijnym porządku prawnym jest niedopuszczalne, gdyż prowadzi do arbitralności i naruszenia zasady pewności prawa. Tego rodzaju konstrukcja, polegająca na zbyt ogólnym określeniu przesłanek, była wielokrotnie krytykowana przez Trybunał Sprawiedliwości UE, który wskazywał, że ograniczenia swobód rynku wewnętrznego muszą być stosowane w sposób ścisły i oparty na jednoznacznych kryteriach⁴¹.

47. Pionowa niezgodność projektu z prawem unijnym uwidacznia się także w tym, że ustawa ingeruje w sfery chronione przez traktatowe swobody gospodarcze oraz przez Kartę Praw Podstawowych. Instytucja poleceń zabezpieczających, przewidziana w projekcie jako instrument umożliwiający nakładanie obowiązków na praktycznie każdy podmiot w sytuacji incydentu krytycznego, może naruszać swobodę prowadzenia działalności gospodarczej oraz prawo własności. Brak precyzyjnych ograniczeń co do zakresu i treści nakładanych obowiązków sprawia, że środek ten może być stosowany w sposób arbitralny. W unijnym porządku prawnym ograniczenia praw podstawowych mogą być wprowadzane wyłącznie w sposób proporcjonalny, konieczny i oparty na jasnych kryteriach. Projektowana regulacja tego standardu nie spełnia. Warto w tym miejscu wskazać, że stanowisko to zostało także wyrażone przez przedstawicieli doktryny⁴².
48. Najbardziej jaskrawym przykładem pionowej niezgodności jest fakt, że Projekt Ustawy rozciąga reżim bezpieczeństwa na wszystkie elementy infrastruktury ICT, traktując je jako równie krytyczne. Tymczasem Dyrektywa NIS2 nakazuje zróżnicowanie podejścia zależnie od krytyczności, ryzyka i funkcji danego elementu systemu. Włączenie do reżimu dostawców wysokiego ryzyka elementów pasywnych, standardowych komponentów sieci stacjonarnych czy mobilnych, a także sprzętu, który w praktyce nie generuje istotnego ryzyka systemowego, jest sprzeczne z zasadą proporcjonalności, zasadą dowodowego uzasadnienia środków oraz zasadą minimalnej ingerencji. Skutkiem Projektu Ustaw jest nie tylko nadregulacja, lecz także deformacja logiki przyjętej w treści Dyrektywy NIS2, która zakłada, że każdy sektor i każdy zasób technologiczny powinien być oceniany przez pryzmat rzeczywistego ryzyka, a nie jego abstrakcyjnej możliwości.

⁴¹ Tak np.: Wyrok TSUE z 26 lutego 2019 r., w sprawie o sygn. C-135/17, X GmbH przeciwko Finanzamt Stuttgart - Körperschaften, wyrok TSUE z 11 września 2008 r., Eckelkamp i in., w sprawie o sygn. C-11/07, ECLI:EU:C:2008:489, pkt 57; wyrok TSUE z 10 lutego 2011 r., Haribo Lakritzen Hans Riegel i Österreichische Salinen, w sprawie o sygn. C-436/08 i C-437/08, ECLI:EU:C:2011:61, pkt 56; wyrok TSUE z 10 kwietnia 2014 r., Emerging Markets Series of DFA Investment Trust Company, w sprawie o sygn. C-190/12, ECLI:EU:C:2014:249, pkt 55.

⁴² Tak np.: M. Górski, Przepisy o cyberbezpieczeństwie budzą wiele wątpliwości, <https://www.rp.pl/polityka/art41459811-prof-marcin-gorski-przepisy-o-cyberbezpieczenstwie-budza-wiele-watpliwosci> (data dostępu: 02.12.2025 r.).

49. W rezultacie Projekt Ustawy - deklarując implementację Dyrektywy NIS2 - w rzeczywistości tworzy system regulacyjny, który wykracza daleko poza ramy tejże Dyrektywy NIS2, ignoruje jej strukturę celów i narusza zasady prawa wyższego rzędu. *Gold-plating* jest dopuszczalny tylko wtedy, gdy jest oparty na faktach, proporcjonalny i zgodny z porządkiem prawnym Unii. W analizowanym Projekcie Ustawy żaden z tych warunków nie został spełniony. Zamiast tego powstała regulacja, która obciąża podmioty licznymi obowiązkami, wprowadza środki o charakterze sankcyjnym bez adekwatnego uzasadnienia, a jednocześnie narusza zasady jednolitego rynku oraz prawa podstawowe. To nie tylko przykład nadregulacji⁴³, lecz przede wszystkim przejaw pionowej niezgodności z prawem unijnym, który podważa skuteczność i prawidłowość implementacji Dyrektywy NIS2 w polskim porządku prawnym.
50. Choć projektodawca powołuje się na unijne podstawy prawne - przede wszystkim Dyrektywę NIS2 oraz wynikające z niej obowiązki implementacyjne - to zasadnicza konstrukcja projektu nie respektuje granic wyznaczonych państwom członkowskim przez prawo Unii Europejskiej i w sposób istotny narusza równowagę pomiędzy krajową swobodą regulacyjną a nadrzędnymi zasadami funkcjonowania rynku wewnętrznego. W rezultacie Projekt Ustawy nie tylko wykracza poza dopuszczalne pole regulacyjne, ale czyni to w sposób, który może prowadzić do pionowej niezgodności - a więc sprzeczności prawa krajowego z przepisami i zasadami unijnymi, które wiążą państwo członkowskie wprost.
51. Podstawowym źródłem tej niezgodności jest brak spełnienia unijnych wymogów płynących z przedstawionej powyżej zasady proporcjonalności, na których opiera się cały system swobód rynku wewnętrznego. Swobody te - swoboda świadczenia usług, swoboda przedsiębiorczości oraz swoboda przepływu towarów - mogą być ograniczane wyłącznie w zakresie, w jakim jest to konieczne do ochrony wartości nadrzędnych, takich jak bezpieczeństwo publiczne, porządek publiczny czy ochrona zdrowia i życia ludzi. Jednakże państwa członkowskie nie mają w tym zakresie nieograniczonej swobody. Ich działania muszą pozostawać poddane regule proporcjonalności tak, jak jest ona rozumiana w prawie UE i w orzecznictwie TSUE. To właśnie ta reguła wyznacza minimalne ramy, które muszą zostać zachowane - a których projektowana ustawa nie wypełnia.
52. W kontekście cyberbezpieczeństwa wymogi proporcjonalności są szczególnie rygorystyczne, gdyż sama Dyrektywa NIS2, którą projekt deklaruje wdrożyć, nakłada na państwa członkowskie obowiązek opierania wszelkich środków regulacyjnych na ustalonych faktach, właściwych analizach ryzyka oraz precyzyjnym ustaleniu relacji pomiędzy celem regulacji, zakresem ingerencji i koniecznością podjętych środków.

⁴³ Co przyznało Ministerstwo Cyfryzacji w treści dokumentu „Opracowanie dla Stałego Komitetu Rady Ministrów dotyczące wymogów regulacyjnych zawartych w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)1), które wykraczają poza standardy przyjęte w innych państwach członkowskich Unii Europejskiej”.

Dyrektywa NIS2 nie tylko dopuszcza nadbudowę krajową, lecz jednocześnie ją warunkuje - wymagając, aby nawet w obszarze niezharmonizowanym, państwo działało w sposób proporcjonalny, oparty na dowodach, a tym samym odporny na arbitralność.

53. Tymczasem Projekt Ustawy, sięgając po bardzo daleko idące środki ingerujące w obrót towarami i usługami ICT, nie przedstawia żadnego materiału analitycznego, który pozwalałby ocenić konieczność czy adekwatność proponowanych rozwiązań. Brak jest zarówno wykazania skali i natury zagrożeń, które miałyby uzasadniać tak drastyczną ingerencję, jak i choćby wstępnej oceny, czy przyjęte środki są konieczne w świetle doświadczenia, praktyki rynkowej oraz - co szczególnie istotne w odniesieniu do Dyrektywy NIS2 - specyfiki poszczególnych sektorów. Projekt Ustawy zatem nie tylko nie jest zgodny z zasadą proporcjonalności; on wręcz uniemożliwia ocenę tej zgodności, ponieważ pozbawia ustawodawcę, adresatów regulacji i sądy danych, które pozwalałyby taki test przeprowadzić.
54. W tym miejscu ujawnia się zasadnicza oś pionowej niezgodności: Projekt Ustawy nie używa unijnych podstaw prawnych jako ram, lecz jako pretekstu do wprowadzenia krajowych rozwiązań, które nie spełniają wspólnotowych standardów. Zamiast wdrożyć Dyrektywę NIS2, Projekt Ustawy rozmienna ją na mechanizm o znacznie szerszym zasięgu, obejmującym całą gospodarkę oraz wszelkie technologie ICT, przy jednoczesnym oparciu się na rekomendacjach *soft law*, takich jak 5G Toolbox, które - choć istotne - nie mają charakteru wiążącego. Przyjmując rozwiązania, które czerpią z 5G Toolbox, ale wychodzą poza jego ramy i ignorują wymogi dowodowe oraz proporcjonalnościowe wynikające z Dyrektywy NIS2, Projekt Ustawy wykracza poza pole uznania pozostawione państwom członkowskim. W efekcie dochodzi do klasycznej sytuacji naruszenia zasady lojalnej współpracy, wynikającej z art. 4 ust. 3 Traktatu o Unii Europejskiej⁴⁴, która nakazuje państwom członkowskim podejmowanie wyłącznie takich środków, które nie utrudniają realizacji celów Unii Europejskiej.
55. Na tym tle szczególnie problematyczne jest powoływanie się przez projektodawcę na wyjątek bezpieczeństwa narodowego, określony w art. 4 ust. 2 TUE. Przepis ten musi być interpretowany ściśle - w sposób, który nie pozwala na arbitralne rozszerzanie zakresu bezpieczeństwa narodowego na wszelkie obszary, w których państwo chciałoby stosować instrumenty ograniczające swobody rynku. TSUE wielokrotnie podkreślał, że bezpieczeństwo narodowe nie może być definiowane przez państwa w sposób dowolny, lecz musi pozostawać w zgodzie z prawem Unii Europejskiej oraz z orzecnictwem Trybunału. Dotyczy to zwłaszcza takich sytuacji, w których ingerencja państwa dotyka podmiotów funkcjonujących na rynku wewnętrznym - przedsiębiorców ICT, dostawców sprzętu czy usługodawców.

⁴⁴ Dz. U. z 2004 r. Nr 90, poz. 864/30 ze zm.

56. Orzecznictwo TSUE dostarcza tu jasnych kryteriów. W sprawie Bouchereau⁴⁵ Trybunał wyjaśnił, że ograniczenie swobód rynku wymaga rzeczywistego i dostatecznie poważnego zagrożenia, godzącego w jeden z podstawowych interesów społeczeństwa. W sprawach dotyczących mechanizmów realokacji migrantów TSUE podkreślił, że państwa członkowskie nie mogą interpretować pojęcia bezpieczeństwa publicznego i narodowego w sposób jednostronny, sprzeczny z celem oraz systemem prawa Unii Europejskiej. Wreszcie w sprawie Internationale Handelsgesellschaft⁴⁶ Trybunał jednoznacznie wskazał, że państwo nie może nakładać na podmioty obowiązków dalej idących niż to, co jest absolutnie konieczne dla ochrony uzasadnionego interesu publicznego.
57. Projektowana ustawa nie spełnia żadnego z tych wymogów. Nie przedstawia żadnych dowodów, które pozwalałyby stwierdzić realne, bezpośrednie i konkretne zagrożenie dla bezpieczeństwa państwa w zakresie, który uzasadniałby tak rozległą ingerencję w swobody rynku wewnętrznego. Zamiast tego odwołuje się do szerokich, niedookreślonych kategorii ryzyka, które - w braku analizy sektorowej i przedmiotowej - mają charakter blankietowy. W rezultacie nie tylko nie można ocenić ich adekwatności, lecz również istnieje ryzyko, że staną się one narzędziem arbitralnego wkraczania w działalność gospodarczą, co pozostaje w sprzeczności z art. 16 i art. 17 Karty Praw Podstawowych⁴⁷, gwarantujących swobodę prowadzenia działalności i ochronę własności.
58. Analiza Projektu Ustawy wskazuje, że przewidziane w nim ograniczenia swobód rynku wewnętrznego i własności nie mieszczą się w ramach przewidzianych przez prawo Unii Europejskiej. Choć Dyrektywa NIS2 przewiduje możliwość tzw. *gold-platingu* poprzez przyjęcie surowszych przepisów krajowych niż wymogi określone w Dyrektywie NIS2, polski mechanizm określania „dostawców wysokiego ryzyka” wydaje się wykraczać poza dopuszczalne granice tej elastyczności. W istotny sposób ingeruje on w swobody rynku wewnętrznego oraz prawo własności, nie spełniając jednocześnie wymogów proporcjonalności i odbiegając zarówno pod względem struktury, jak i intensywności od środków przewidzianych w Dyrektywie NIS2. Rozszerzenie zakresu podmiotowo-przedmiotowego, wprowadzenie surowszych sankcji oraz rygorystycznych ograniczeń proceduralnych sprawia, że realizacja niektórych decyzji może w praktyce utrudniać skuteczną kontrolę sądową, zwiększając ryzyko naruszenia prawa Unii Europejskiej.
59. Dyrektywa NIS2 stanowi harmonizację minimalną, umożliwiając państwom członkowskim wprowadzanie bardziej rygorystycznych regulacji, pod warunkiem że pozostają one zgodne z obowiązkami wynikającymi z Traktatu o Funkcjonowaniu Unii

⁴⁵ Wyrok TSUE z dnia 27 października 1977 r., w sprawie o sygn. 30-77, Régina (UK) v Pierre Bouchereau, Zbiór orzeczeń Europejskiego Trybunału Sprawiedliwości 1977 - 01999, ECLI:EU:C:1977:172.

⁴⁶ Wyrok TSUE z dnia 17 grudnia 1970 r., Internationale Handelsgesellschaft mbH przeciwko Einfuhr- und Vorratsstelle für Getreide und Futtermittel, w sprawie o sygn. 11-70, ECLI:EU:C:1970:114.

⁴⁷ Por. szerzej np.: A. Barczak, A. Kaźmierska-Patrzyzna, Prawo własności jako konstytucyjne prawo podmiotowe a zasada proporcjonalności - zagadnienia administracyjnoprawne, St.Prawn.KUL 2025, nr 1, s. 23-36.

Europejskiej oraz z Kartą Praw Podstawowych UE. W konsekwencji każde krajowe rozwiązanie dotyczące dostawców wysokiego ryzyka nie może być traktowane jako „czysto krajowe”, lecz podlega ocenie w kontekście zgodności z zasadami swobodnego przepływu towarów wynikającej z art. 26 ust. 2 TFUE⁴⁸, swobody przedsiębiorczości lub świadczenia usług⁴⁹ oraz ochrony własności. Ograniczenia tych swobód mogą być wprowadzane wyłącznie w drodze ustawowej, w interesie publicznym, przy zachowaniu proporcjonalności środków względem osiąganego celu⁵⁰.

60. Analiza Projektu Ustawy prowadzi do wniosku, iż obarczony jest on wieloma sprzecznościami i uchybieniami. Przepisy Projektu Ustawy przewidujące zakaz wprowadzania do użytkowania lub nakaz wycofania określonych produktów ICT oraz ograniczenia nabywania wybranych produktów przez zamawiających mają charakter środków o skutku równoważnym do ograniczeń ilościowych, ograniczając swobodny przepływ towarów i dostęp do rynku krajowego. Projekt Ustawy nie zawiera rzetelnych dowodów ani analiz, które mogłyby uzasadnić konieczność zastosowania takich restrykcji oraz potwierdzić ich proporcjonalność.
61. Równie istotne ograniczenia dotyczą swobody przedsiębiorczości i świadczenia usług. Zakazy wprowadzania określonych rodzajów usług ICT oraz rygor natychmiastowej wykonalności decyzji w przypadku dotyczącym dostawców wysokiego ryzyka znacząco ograniczają możliwość prowadzenia działalności gospodarczej i korzystania z atrybutów własności. Brak przewidzianych rozpraw, ograniczony dostęp do pełnego uzasadnienia decyzji oraz natychmiastowa wykonalność nakazów zwiększają ciężar regulacyjny dla przedsiębiorców, utrudniając w praktyce skuteczną obronę przed decyzjami administracyjnymi.
62. Kolejnym problemem są przepisy nakazujące wycofanie produktów ICT w okresie krótszym niż ich faktyczny okres użytkowania, co ingeruje w prawo własności chronione art. 17 Karty Praw Podstawowych. Projekt Ustawy, jak również jego uzasadnienie⁵¹ nie wykazuje, że mniej restrykcyjne środki, takie jak działania naprawcze, środki tymczasowe lub łagodniejsze ograniczenia, nie byłyby wystarczające do osiągnięcia celów bezpieczeństwa, co podważa zasadę proporcjonalności.
63. Mechanizm przyjęty na gruncie Projektu Ustawy odnoszący się do dostawców wysokiego ryzyka odbiega również od standardu wprowadzonego w treści Dyrektywy NIS2 w zakresie charakteru i skali stosowanych środków. Zamiast wprowadzać działania

⁴⁸ Por. szerzej np.: J. Galster, C. Mik, Podstawy europejskiego prawa wspólnotowego - zarys wykładu, Toruń 1996.

⁴⁹ Wynikających z art. 46 i art. 56 TFUE.

⁵⁰ Por. szerzej: Wyrok TSUE z dnia 19 czerwca 2025 r., w sprawie C-200/24 Komisja Europejska przeciwko Rzeczypospolitej Polskiej; wyrok dostępny jest pod adresem internetowym: [CURIA - Documents](https://eur-lex.europa.eu/curia/doclist/curia.do?method=docsList&docid=864888) (data dostępu: 02 grudnia 2025 r.).

⁵¹ Uzasadnienie rządowego projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Druk nr 1955, dostępny na stronie internetowej pod adresem: <https://www.sejm.gov.pl/sejm10.nsf/druk.xsp?nr=1955> (data dostępu: 02.12.2025 r.).

tymczasowe i sekwencyjne - od ostrzeżeń, poprzez polecenia naprawcze i audyty, aż po zawieszenia lub zakazy jako *ultima ratio* - projekt przewiduje natychmiastowe i definitywne nakazy oraz zakazy, bez przekonującego uzasadnienia konieczności ich zastosowania. Zakres podmiotowo-przedmiotowy jest nadmierny, obejmując wszystkie sektory i wszystkie kategorie ICT, podczas gdy Dyrektywa NIS2 koncentruje środki na krytycznych łańcuchach dostaw w oparciu o skoordynowane oceny ryzyka na poziomie UE.

64. Dodatkowo przewidziane sankcje administracyjne mogą być wielokrotnie wyższe niż minimalne pułapy określone w Dyrektywy NIS2, a ograniczenia proceduralne - brak rozpraw, rygor natychmiastowej wykonalności decyzji czy ograniczony dostęp do uzasadnienia wyroków - mogą uniemożliwiać skuteczną kontrolę sądową⁵², w praktyce pogłębiając ingerencję w swobody i prawa podmiotów.
65. Podsumowując, projekt mechanizmu określania „dostawców wysokiego ryzyka” w obecnym kształcie narusza art. 34-36 TFUE (swobodny przepływ towarów), art. 49-55 TFUE oraz art. 56-62 TFUE i art. 16 Karty Praw Podstawowych (swoboda przedsiębiorczości i świadczenia usług), art. 17 Karty Praw Podstawowych (prawo własności), a także zasadę proporcjonalności przewidzianą w Dyrektywie NIS2. Nieprawidłowości te wynikają z nadmiernie restrykcyjnych, często definitywnych środków, braku wykazania konieczności ich zastosowania, nadmiernie szerokiego zakresu podmiotowo-przedmiotowego, nieadekwatnie wysokich kar oraz ograniczeń proceduralnych utrudniających skuteczną kontrolę sądową. Aby zapewnić zgodność z prawem UE, konieczne byłoby wprowadzenie sekwencyjności i tymczasowości środków, ograniczenie ich stosowania do krytycznych łańcuchów dostaw po dokonaniu skoordynowanej oceny ryzyka na poziomie Unii Europejskiej, dostosowanie sankcji do standardów Dyrektywy NIS2 oraz złagodzenie ograniczeń proceduralnych w sposób gwarantujący efektywną kontrolę sądową.
66. Przepisy Projektu Ustawy dotyczące uznawania dostawców ICT za podmioty wysokiego ryzyka nakładają zarówno zakaz wprowadzania do użytkowania określonych typów produktów i usług, jak i obowiązek ich wycofania oraz zakaz nabywania ich przez zamawiających. Oznacza to bezpośrednie ograniczenie swobody przepływu towarów, swobody przedsiębiorczości oraz prawa własności. Nawet jeśli przepisy nie mają charakteru dyskryminującego wprost, ich skutki praktyczne prowadzą do znaczącego utrudnienia dostępu produktów ICT pochodzących z innych państw członkowskich Unii Europejskiej do polskiego rynku, czyniąc działalność przedsiębiorstw mniej atrakcyjną i ograniczając możliwość korzystania z własności w pełnym zakresie.

⁵² Por. szerzej: P. Wajda, A. Wiktorowska, Kontrola sądowa administracji publicznej [w:] J. Jagielski (red.), M. Wierzbowski (red.), Prawo administracyjne, Warszawa 2019, s. 337; zob. także: Wyrok TK z dnia 9 czerwca 1998 r.; sygnatura: K 28/97; Legalis; Wyrok TK z dnia 4 lipca 2002 r.; sygnatura: P 12/01; Legalis; Wyrok TK z dnia 15 stycznia 2007 r.; sygnatura: P 19/06; Legalis.

67. Pod względem proporcjonalności środki przyjęte w projekcie ustawy są nieadekwatne i nadmierne. Dyrektywa NIS2, której Projekt Ustawy formalnie deklaruje implementację, nie przewiduje ani pojęcia dostawcy wysokiego ryzyka, ani obowiązku wycofywania sprzętu lub oprogramowania z użytkowania w sposób natychmiastowy i powszechny. Dyrektywa NIS2 określa ramy implementacyjne dla państw członkowskich w sposób precyzyjny, w tym wymaga, aby środki przyjmowane w sferze regulacji zharmonizowanej i niezharmonizowanej były oparte na analizie faktycznej, adekwatne i proporcjonalne w odniesieniu do konkretnego ryzyka dla funkcjonowania systemów i sektorów gospodarki. Procedura przewidziana w Projekcie Ustawy, obejmująca możliwość natychmiastowej wykonalności decyzji, ograniczenie prawa do rozprawy, doręczenie tylko częściowego uzasadnienia wyroku oraz brak wymogu przeprowadzenia analizy ryzyka i krytyczności zasobów, uniemożliwia rzetelną ocenę zgodności z zasadą proporcjonalności, a tym samym narusza wymogi prawa unijnego.
68. Projekt ustawy wprowadza nadregulację również poprzez rozciągnięcie implementacji rekomendacji Unii Europejskiej zawartych w 5G Toolbox, które w świetle art. 288 TFUE mają charakter *soft law* i nie stanowią obowiązującego prawa. Włączenie tych zaleceń jako podstawy prawnej krajowej regulacji powoduje, że Polska przyjęła środki o charakterze bardziej rygorystycznym niż przewiduje to Dyrektywa NIS2. 5G Toolbox pierwotnie odnosił się jedynie do sektora telekomunikacyjnego, w szczególności do dostawców infrastruktury 5G, i miał charakter zaleceniowy, mający wspierać państwa członkowskie w opracowywaniu środków zarządzania ryzykiem. Tymczasem Projekt Ustawy rozszerza zakres jego zastosowania na wszystkie 18 sektorów wymienionych w NIS2, w tym energetykę, sektor finansowy, ochronę zdrowia, transport, gospodarkę wodną, odpadową i chemiczną⁵³, co wykracza poza jakiekolwiek praktyki przyjęte w innych państwach członkowskich. Żadne państwo Unii Europejskiej nie wprowadziło tak szerokich środków, a tylko nieliczne ograniczenia odnoszą się do sektora telekomunikacyjnego i obejmują ograniczenia wprowadzania do użytkowania lub wycofywania sprzętu i oprogramowania po analizie krytyczności zasobów i możliwości wprowadzenia środków naprawczych.
69. Nadmierny charakter regulacji widać również w porównaniu do kar przewidzianych w Dyrektywie NIS2. Dyrektywa NIS2 określa administracyjne sankcje dla podmiotów kluczowych i ważnych, które mają być skuteczne, proporcjonalne i odstrasżające, lecz nie przewiduje kar przekraczających 10 milionów euro lub 2% rocznego obrotu dla podmiotów kluczowych. Projekt Ustawy natomiast przewiduje kary do 100 milionów złotych, co w wielu przypadkach oznacza ponad dwukrotne przekroczenie poziomów unijnych. Uzasadnienie projektowanych kar odnosi się jedynie do obecnych krajowych przepisów i ryzyk wynikających z sytuacji międzynarodowej, nie zaś do wymogów Dyrektywy NIS2

⁵³ Por. np.: <https://www.pwc.pl/pl/uslugi/nis2-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html> (data dostępu: 02.12.2025 r.).

ani do przeprowadzonych analiz proporcjonalności wobec rynku wewnętrznego Unii Europejskiej.

70. Procedury wynikające z art. 67b-67c Projektu Ustawy stanowią kolejne naruszenie zasady proporcjonalności i mogą ograniczać swobodę przedsiębiorczości. W sytuacji, gdy minister zakwalifikuje sprzęt lub oprogramowanie jako niebezpieczne, przedsiębiorca musi wstrzymać dystrybucję, co może skutkować utratą przychodów i dodatkowych kosztów, nawet jeśli decyzja okaże się bezprawna w późniejszym postępowaniu sądowym. Doręczenie wyroku z częściowym uzasadnieniem uniemożliwia skuteczne zaskarżenie decyzji, a brak analizy krytyczności zasobów i ryzyka powoduje, że ograniczenia obejmują wszystkie produkty i procesy w danym sektorze, niezależnie od faktycznego zagrożenia dla bezpieczeństwa państwa.
71. W rezultacie Projekt Ustawy wprowadza regulacje nieproporcjonalne, nadmierne i pionowo niezgodne z prawem Unii Europejskiej, zarówno w zakresie implementacji Dyrektywy NIS2, jak i w odniesieniu do zasad rynku wewnętrznego, swobody przedsiębiorczości i prawa własności. Rozszerzenie obowiązków wynikających z 5G Toolbox do rangi obowiązującego prawa krajowego, rozciągnięcie ograniczeń na wszystkie sektory objęte zakresem zastosowania przepisów Dyrektywy NIS2, brak procedury stopniowego zarządzania ryzykiem oraz nadmierne sankcje finansowe stanowią przykład legislacji wykraczającej poza dopuszczalne ramy krajowego uznania, przewidziane w art. 4 TUE, art. 36 i 52 TFUE oraz w art. 17 Karty Praw Podstawowych.
72. W konsekwencji Projekt Ustawy w obecnym kształcie nie spełnia wymogów proporcjonalności, wprowadza nadregulację w stosunku do prawa Unii Europejskiej⁵⁴ i ryzyka, które ma chronić, a w praktyce może prowadzić do ograniczenia konkurencyjności przedsiębiorstw oraz zakłócenia swobodnego przepływu towarów i usług na rynku wewnętrznym Unii Europejskiej⁵⁵.

III.4. Zgodność Projektu Ustawy z Konstytucją RP.

73. W pierwszej kolejności należy wskazać, że projektowany art. 67b ust. 15 Projekt Ustawy, będącej przedmiotem niniejszej analizy, wprowadza mechanizm kwalifikowania określonych dostawców sprzętu lub oprogramowania jako tzw. dostawców wysokiego ryzyka, przy czym kwalifikacja ta dokonywana jest - w drodze decyzji administracyjnej - przez ministra właściwego do spraw informatyzacji. Konstrukcja ta opiera się na założeniu,

⁵⁴ Zob. szerzej: T. Siemiątkowski, Szkodliwa nadregulacja w sprawie cyberbezpieczeństwa, dostęp: <https://www.rp.pl/opinie-prawne/art41473571-prof-tomasz-siemiatkowski-szkodliwa-nadregulacja-w-sprawie-cyberbezpieczenstwa> (data dostępu: 02.12.2025 r.).

⁵⁵ Por.: Certyfikacja zamiast blokowania – to odpowiedź na zmianę prawa, dostęp: <https://cyfrowa-gospodarka.gazetaprawna.pl/biznes/9506680,certyfikacja-zamiast-blokowania-to-odpowiedz-na-zmiane-prawa.html> (data dostępu: 02.12.2025 r.).

że dostawca taki może stanowić zagrożenie dla podstawowego interesu bezpieczeństwa państwa, co ustawodawca uznaje za przesłankę wystarczającą do podjęcia daleko idącej ingerencji w sferę działalności gospodarczej podmiotów krajowych.

74. Projektowane brzmienie art. 67b ust. 16 Projektu Ustawy dopełnia tej regulacji, określając elementy obligatoryjne takiej decyzji, w szczególności zaś wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT objętych zakresem postępowania. Konstrukcja ta, choć formalnie przewiduje katalog otwarty, w praktyce otwiera możliwość szerokiego i nie do końca zdefiniowanego zakresu ingerencji w działalność gospodarczą podmiotów objętych decyzją.
75. W dalszej kolejności należy odnieść się do skutków prawnych decyzji ministra, jakie projekt wiąże z uznaniem dostawcy za dostawcę wysokiego ryzyka. Zgodnie z art. 67c ust. 1 Projektu Ustawy, obowiązek usunięcia z użytkowania - bądź powstrzymania się od wprowadzania do użytkowania - określonych typów produktów, usług lub procesów ICT zostaje nałożony na podmioty kluczowe i ważne oraz na przedsiębiorców telekomunikacyjnych, których przychód z tytułu działalności telekomunikacyjnej przekroczył w poprzednim roku obrotowym kwotę 10 milionów złotych.
76. Projekt Ustawy przewiduje przy tym dwa odrębne terminy realizacji obowiązku wycofania produktów: siedmioletni dla podmiotów kluczowych i ważnych oraz czteroletni dla przedsiębiorców telekomunikacyjnych określonych w art. 67b ust. 1 Projektu Ustawy. Jednocześnie ustawodawca wprost wyłącza możliwość dochodzenia jakiegokolwiek odszkodowania z tytułu poniesionych kosztów. Zabieg ten należy postrzegać jako wprowadzenie środka o charakterze szczególnie dolegliwym, bowiem ingeruje on nie tylko w swobodę prowadzenia działalności gospodarczej, lecz także w sferę majątkową przedsiębiorców⁵⁶, przerzucając na nich pełen ciężar ekonomiczny wdrażanych decyzji.
77. Analizy wymaga również kwestia udziału przedsiębiorców w postępowaniu dotyczącym uznania dostawcy za dostawcę wysokiego ryzyka. Projekt Ustawy przewiduje bowiem, że w postępowaniu tym - poza samym dostawcą - mogą uczestniczyć jedynie przedsiębiorcy komunikacji elektronicznej, których przychód w poprzednim roku obrotowym wyniósł co najmniej dwudziestotysięczną krotność przeciętnego wynagrodzenia ogłaszanego przez Prezesa GUS. Oznacza to, że przedsiębiorcy osiągający roczny przychód przekraczający 10 milionów złotych, lecz niemieszczący się w drugim, znacznie wyższym progu, zostają *de facto* pozbawieni możliwości obrony swoich interesów w postępowaniu, którego efektem będzie późniejsze nałożenie na nich obowiązku usunięcia z użytkowania określonych produktów lub usług ICT. Powstaje w ten sposób asymetria proceduralna, prowadząca do zróżnicowania sytuacji podmiotów podobnych pod względem materialnym, lecz arbitralnie rozdzielonych na podstawie kryterium ekonomicznego.

⁵⁶ Por. szerzej: B. Banaszak, *Prawo konstytucyjne*, Warszawa 2008, s. 245; zob. także: Wyrok NSA z dnia 14 czerwca 2007 r.; sygnatura: I OSK 717/06; LEX nr 354713.

78. Tak ukształtowany mechanizm, w świetle standardów wynikających z art. 2 Konstytucji RP, budzi poważne zastrzeżenia pod kątem zasad proporcjonalności i zaufania obywateli do państwa oraz stanowionego przez nie prawa⁵⁷. Projektowane rozwiązania prowadzą bowiem do nadmiernej ingerencji w sferę praw majątkowych i swobody działalności gospodarczej, nie poprzedzając tych działań adekwatnymi gwarancjami proceduralnymi oraz nie wykazując, że przedsięwzięcie to jest konieczne i niezbędne dla osiągnięcia zakładanego celu regulacyjnego. Co więcej, ustawodawca, powołując się na zagrożenia wynikające z rozwoju technologii oraz ograniczoną zdolność państwa do zapobiegania incydentom krytycznym, przerzuca ciężar zapewnienia bezpieczeństwa państwa na podmioty prywatne, jednocześnie eliminując możliwość uzyskania przez nie rekompensaty oraz ograniczając ich udział w procedurze decyzyjnej.
79. W uzasadnieniu projektu ustawodawca podkreśla, że przedsiębiorcy telekomunikacyjni oraz dostawcy usług zaufania nie są obecnie podmiotami krajowego systemu cyberbezpieczeństwa, a państwo nie posiada wystarczających instrumentów prawnych pozwalających na skuteczną reakcję na incydent krytyczny. Z tego twierdzenia wywodzi następnie konieczność rozszerzenia obowiązków tych podmiotów i przyznania organom państwowym daleko idących kompetencji nadzorczych. Regulacja ta prowadzi jednak do swoistego „upaństwowienia” podmiotów prywatnych w zakresie wykonywanej przez nie działalności, gdyż zobowiązuje je do działań służących realizacji celów publicznych, a jednocześnie pozbawia możliwości wpływania na proces legislacyjny oraz ochrony swoich interesów w toku postępowania administracyjnego.
80. Wreszcie, nie sposób pominąć kwestii proporcjonalności środka wprowadzanego przez ustawodawcę. Nakaz wycofania z użytkowania infrastruktury ICT - często o strategicznym znaczeniu dla funkcjonowania przedsiębiorcy - stanowi środek o charakterze drastycznym, ingerujący jednocześnie w stabilność ekonomiczną podmiotów, w ciągłość świadczonych usług oraz w ład kontraktowy. Tymczasem projekt nie wykazuje, że środki mniej uciążliwe (np. zwiększony nadzór, ograniczone wykorzystanie, obowiązki sprawozdawcze) byłyby niewystarczające dla osiągnięcia celu regulacji. Takie ukształtowanie instrumentu sankcyjnego pozostaje w sprzeczności z utrwalonym w orzecznictwie Trybunału Konstytucyjnego rozumieniem zasady przyzwoitej legislacji, obejmującej wymóg proporcjonalności, adekwatności i konieczności.
81. Ocena proporcjonalności, będąca jednym z fundamentów kontroli konstytucyjnej w demokratycznym państwie prawnym, została w utrwalonym orzecznictwie Trybunału Konstytucyjnego ujęta jako procedura trójelementowa, mająca na celu ustalenie, czy wprowadzona regulacja ustawowa odpowiada standardom wynikającym z art. 2

⁵⁷ Zob.: P. Tuleja, *Komentarz do art. 2 Konstytucji RP*, [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP. Tom I. Komentarz do art. 1-86*, Warszawa 2016, Nb. 45; por. także: postanowienie NSA z dnia 6 czerwca 2019 r.; sygnatura: II OSK 166/18; Legalis; wyrok NSA z dnia 25 września 2024 r.; sygnatura: III OSK 1038/23; Legalis; Wyrok NSA z dnia 25 września 2024 r.; sygnatura: III OSK 1039/23; Legalis; wyrok NSA z dnia 4 kwietnia 2023 r.; sygnatura: II FSK 255/22; Legalis; wyrok NSA z dnia 12 grudnia 2022 r.; sygnatura II GSK 468/22; Legalis.

Konstytucji RP. Trybunał przyjął bowiem, że analiza ta powinna udzielać odpowiedzi na trzy kluczowe pytania: po pierwsze - czy dane rozwiązanie normatywne jest zdolne doprowadzić do osiągnięcia zamierzonego przez ustawodawcę celu (kryterium przydatności); po drugie - czy środek zastosowany w regulacji jest niezbędny dla ochrony określonego interesu publicznego, a więc czy nie istnieją inne, mniej dolegliwe instrumenty prawne umożliwiające realizację tego celu (kryterium konieczności); po trzecie wreszcie - czy ciężary nakładane na jednostkę pozostają w proporcji do spodziewanych korzyści regulacyjnych, co stanowi istotę proporcjonalności sensu stricto. W świetle tej metodologii Trybunał podkreśla, że art. 2 Konstytucji RP jest nie tylko normatywnym wyrazem zasady demokratycznego państwa prawnego, lecz także samodzielnym źródłem zasady proporcjonalności, mogącej stanowić wyłączny wzorzec kontroli w postępowaniu przed Trybunałem.

82. Ustalając zgodność projektowanych przepisów z zasadą proporcjonalności, należy zatem odnieść ocenę do trzech wspomnianych płaszczyzn. Rozwiązanie przyjęte w opiniowanej regulacji - polegające na nakazie usunięcia sprzętu lub oprogramowania dostawcy uznanego za dostawcę wysokiego ryzyka, bez przyznania podmiotom objętym decyzją prawa do odszkodowania - niewątpliwie może doprowadzić do realizacji zamierzonego celu, jakim jest eliminacja potencjalnych zagrożeń dla bezpieczeństwa państwa. Nie jest to jednak środek niezbędny. Z perspektywy dostępnych instrumentów prawnych i technicznych istnieją bowiem rozwiązania o nieporównywalnie niższym stopniu ingerencji w sferę praw majątkowych i wolności działalności gospodarczej, takie jak rozwinięte mechanizmy certyfikacji cyberbezpieczeństwa, obowiązki audytowe czy dywersyfikacja dostawców ICT. Środki te, choć mniej dolegliwe, mogą w sposób równoważny - a niekiedy bardziej precyzyjny - zapewnić bezpieczeństwo systemów teleinformatycznych bez konieczności stosowania sankcji o charakterze *quasi*-wywłaszczeniowym.
83. W konsekwencji należy uznać, że ciężary nakładane na przedsiębiorców przez projektowaną regulację pozostają w rażącej dysproporcji do zakładanych efektów. Dolegliwość środka - w postaci przymusowego usunięcia infrastruktury ICT oraz obciążenia przedsiębiorcy pełnym kosztem tej operacji - wykracza poza zakres konieczny do osiągnięcia celu regulacyjnego. Tym samym rozwiązanie to narusza standard proporcjonalności sensu stricto, a przez to pozostaje w sprzeczności z wymaganiami wynikającymi z art. 2 Konstytucji RP.
84. Naruszenie zasady proporcjonalności rodzi również dalsze konsekwencje systemowe. W orzecznictwie Trybunału Konstytucyjnego konsekwentnie podkreśla się, że jednym z filarów demokratycznego państwa prawnego jest zasada racjonalności ustawodawcy, której treść wywodzi się właśnie z art. 2 Konstytucji RP. Państwo prawa opiera się bowiem na założeniu, że stanowione normy prawne są rezultatem przemyślanego procesu legislacyjnego, opartego na analizie skutków regulacji oraz wyważeniu wartości konstytucyjnych. Trybunał akcentuje, że racjonalizm stanowienia prawa nie jest jedynie

postulatem teoretycznym, lecz fikcją prawną o fundamentalnym znaczeniu dla stabilności systemu prawnego. Gdyby bowiem przyjąć, że ustawodawca działa w sposób arbitralny bądź nieprzemyślany, wówczas każdy akt prawny mógłby być podważany, co prowadziłoby do erozji zaufania obywateli do państwa oraz do dezintegracji więzi społecznych.

85. Tymczasem projektowane przepisy, wprowadzając mechanizmy dalece ingerujące w sferę własności prywatnej i wolności działalności gospodarczej, bez wykazania konieczności zastosowania środka o takim stopniu dolegliwości, podważają założenie racjonalności ustawodawcy. W świetle utrwalonej linii orzeczniczej Trybunału działania legislacyja muszą pozostawać w zgodzie z regułami przyzwoitej legislacji, do których zalicza się również racjonalność przyjmowanych rozwiązań prawnych. Nieproporcjonalność opiniowanych przepisów prowadzi zatem do ich niezgodności nie tylko z zasadą proporcjonalności, ale również z zasadą racjonalności ustawodawcy, stanowiącą integralny element art. 2 Konstytucji RP.
86. Niezależnie od powyższego, projektowana regulacja wkracza także w obszar konstytucyjnie chronionych zasad ustroju gospodarczego, w szczególności zasady społecznej gospodarki rynkowej wyrażonej w art. 20 Konstytucji RP. Trybunał Konstytucyjny wielokrotnie wskazywał, że uczynienie własności prywatnej jednym z podstawowych elementów ustroju gospodarczego jest wyrazem jednoznacznego odejścia od modelu, w którym dominowała własność państwowa oraz własność podmiotów powiązanych z państwem⁵⁸. Projektowane rozwiązanie - poprzez daleko idące powiązanie podmiotów prywatnych z realizacją celów publicznych, bez odpowiednich gwarancji prawnych - prowadzi do naruszenia tej zasady, wprowadzając nadmierne, nieuzasadnione konstytucyjnie ograniczenia w sferze wolności gospodarczej.
87. Szczególnie problematyczne jest w tym kontekście pozbawienie przedsiębiorców prawa do odszkodowania z tytułu przymusowego usunięcia sprzętu lub oprogramowania. W świetle art. 21 ust. 2 Konstytucji RP wywłaszczenie - rozumiane szeroko jako każde przymusowe pozbawienie lub ograniczenie praw majątkowych⁵⁹ - jest dopuszczalne wyłącznie wówczas, gdy następuje na cele publiczne i za słusznym odszkodowaniem⁶⁰. Z orzecnictwa Trybunału wynika, że wywłaszczenie może przybrać formę zarówno aktu indywidualnego, jak i generalnego, o ile jego skutkiem jest faktyczne pozbawienie jednostki prawa majątkowego⁶¹. Nakaz trwałego usunięcia określonych produktów ICT - bez jakiegokolwiek kompensacji - spełnia wszelkie cechy wywłaszczenia *sensu largo*,

⁵⁸ Por. szerzej: Wyrok TK z 21.03.2000 r., K 14/99, OTK 2000, nr 2, poz. 61; L. Garlicki, Polskie prawo konstytucyjne, Warszawa 1999, s. 82.

⁵⁹ Por. szerzej: Wyrok TK z 12.12.2017 r., SK 39/15, OTK-A 2017, nr 86.

⁶⁰ Por. także: Postanowienie SN z dnia 24 stycznia 2024 r.; sygnatura: II KK 400/23; LEX nr 3658273.

⁶¹ Por. szerzej: P. Tuleja [w:] P. Tuleja, red., Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warszawa 2019, s. 91.

prowadząc do eliminacji elementów majątku przedsiębiorcy i naruszenia struktury jego zasobów technicznych.

88. W powyższym kontekście warto przypomnieć, że choć prawo własności, nawet jako jedno z najsilniej chronionych praw majątkowych, nie ma charakteru absolutnego, to ograniczenia tego prawa muszą mieścić się w granicach wyznaczonych Konstytucją RP, zaś ingerencja ustawodawcy powinna uwzględniać konieczność ochrony dobra wspólnego oraz innych wartości konstytucyjnych. Ochrona własności nie może zostać sprowadzona do fikcji, a państwo ma pozytywny obowiązek zapewnienia jej realnej efektywności⁶². Oznacza to, że regulacje prowadzące do pozbawienia podmiotów gospodarczych elementów ich majątku - w tym infrastruktury technicznej - bez rekompensaty, naruszają standard ochrony wywodzony zarówno z art. 21 ust. 2 Konstytucji RP, jak i art. 64 Konstytucji RP.
89. Z powyższych względów należy stwierdzić, że projektowane rozwiązanie, ingerując w sposób arbitralny⁶³ i nieproporcjonalny w sferę praw majątkowych oraz wolności działalności gospodarczej podmiotów prywatnych, narusza nie tylko zasadę proporcjonalności i racjonalności ustawodawcy, lecz także fundamentalne zasady ustroju gospodarczego Rzeczypospolitej Polskiej oraz konstytucyjne gwarancje ochrony własności⁶⁴.
90. Ocena regulacji ingerujących w prawo własności - jednego z filarów porządku konstytucyjnego - nigdy nie sprowadza się wyłącznie do suchego stwierdzenia, że ograniczenia są dopuszczalne lub niedopuszczalne. W centrum tej oceny znajduje się bowiem precyzyjna analiza ram konstytucyjnych, które wyznaczają granice, poza które ustawodawca wyjść nie może, nawet jeśli deklarowany cel regulacji wydaje się słuszny czy potrzebny. Właśnie te konstytucyjne ramy decydują o tym, czy ograniczenie prawa własności mieści się jeszcze w dopuszczalnej przestrzeni działania państwa, czy też staje się ingerencją nadmierną - naruszającą istotę chronionego prawa⁶⁵.
91. Konstytucja RP dopuszcza bowiem możliwość wprowadzania ograniczeń prawa własności, lecz jedynie w takim zakresie, w jakim nie prowadzi to do uszczuplenia jego istoty. To zaś pociąga za sobą konieczność przeprowadzenia swoistej triadycznej analizy:

⁶² Postanowienie TK z 6.11.2019 r., SK 21/18, OTK-A 2019, nr 58; Wyrok TK z 24.10.2001 r., SK 22/01, OTK 2001, nr 7, poz. 216.

⁶³ Tak też: K. Klecha, *Wolność działalności gospodarczej w Konstytucji RP*, Warszawa 2009, s. 220; S. Korus, *Ochrona zdrowia jako przejaw ważnego interesu publicznego w rozumieniu art. 22 Konstytucji RP w dobie epidemii choroby COVID-19*, Warszawa 2020, s. 143 i nast.

⁶⁴ Por. szerzej: Wyrok TK z dnia 12 stycznia 1999 r.; sygnatura: P 2/98; Legalis; Wyrok TK z dnia 25 maja 1999 r.; sygnatura: SK 9/98; Legalis; Wyrok TK z dnia 12 stycznia 2000 r.; sygnatura: P 11/98; Legalis; Wyrok TK z dnia 10 października 2000 r.; sygnatura: P 8/99; Legalis.

⁶⁵ Por. szerzej: Wyrok NSA z dnia 11 stycznia 2017 r.; sygnatura: II OSK 932/15; Legalis; Wyrok NSA z dnia 01 czerwca 2012 r.; sygnatura: II OSK 844/12; Legalis; Wyrok TK z dnia 23 października 2012 r.; sygnatura: SK 11/12; Legalis; Wyrok NSA z dnia 12 stycznia 2016 r.; sygnatura: II OSK 1132/14; Legalis; Wyrok NSA z dnia 10 października 2017 r.; sygnatura: II OSK 265/16; Legalis.

rozważyć należy, czy dane rozwiązanie ustawowe jest zdolne do osiągnięcia zakładanych celów; czy stanowi środek rzeczywiście konieczny dla ochrony wartości publicznych, z którymi jest powiązane; wreszcie - czy ciężary nakładane na jednostkę pozostają w słusznej, nienaruszającej równowagi proporcji do zamierzonego rezultatu⁶⁶. W przypadku opiniowanych przepisów Projektu Ustawy, jak już wskazano, egzamin ten nie został zdany: mamy do czynienia z ingerencją nadmierną, wykraczającą poza to, co w demokratycznym państwie prawnym może być uznane za konieczne i dopuszczalne.

92. Ustawodawca, chcąc ingerować w sferę własności, zobowiązany jest do poszanowania wartości konstytucyjnych, wskazanych nie tylko w art. 31 ust. 3 Konstytucji RP, lecz również w innych normach ustawy zasadniczej, które uzupełniają obraz obowiązków państwa wobec jednostki. W myśl tej zasady środki użyte przez prawodawcę mają być adekwatne, racjonalne i nieprzekraczające tego, co absolutnie konieczne dla osiągnięcia zamierzonego dobra wspólnego⁶⁷. Stosując przedstawiony w części II.3 test proporcjonalności, środek polegający na nakazie usunięcia infrastruktury ICT oraz przerzuceniu pełnych kosztów na przedsiębiorcę nie jest niezbędny wobec dostępności mniej dolegliwych instrumentów (certyfikacja, audyt, środki naprawcze, dywersyfikacja dostawców). Bilans korzyści i kosztów pozostaje negatywny, co przesądza o naruszeniu proporcjonalności *sensu stricto* w odniesieniu do prawa własności i wolności działalności gospodarczej.
93. W przypadku prawa własności tę dodatkową ochronę powtarza i wzmacnia art. 64 ust. 3 Konstytucji RP - własność może być ograniczona⁶⁸ wyłącznie w drodze ustawy i tylko w takim zakresie, w jakim nie narusza to istoty prawa własności⁶⁹. Trybunał Konstytucyjny w swoim orzecznictwie wielokrotnie podkreślał, że „istota prawa” oznacza sferę zupełnie nienaruszalną, pewien rdzeń, którego nie wolno dotknąć nawet wtedy, gdy ograniczenie spełnia wszystkie inne przesłanki konstytucyjne. Granicę tę wyznacza funkcja danego prawa w ustroju konstytucyjnym⁷⁰ - funkcja wynikająca z podstawowych zasad systemu,

⁶⁶ Zob. np.: Wyrok NSA z dnia 7 września 2021 r.; sygnatura: III OSK 1035/21; LEX nr 3225418; Wyrok NSA z dnia 19 sierpnia 2021 r.; sygnatura: I FSK 203/21; LEX nr 3245595; Wyrok TK z dnia 12 lutego 2015 r.; sygnatura: SK 70/13, Legalis; por. także: Wyrok TK z dnia 22 września 2005 r.; sygnatura: KP 1/05, OTK-A 2005, Nr 8, poz. 93; Wyrok TK z dnia 22 września 2009 r.; sygnatura: P 46/07, OTK-A 2009, Nr 8A, poz. 126; Wyrok WSA w Rzeszowie z dnia 12 marca 2019 r.; sygnatura: II SA/Rz dnia 1411/18; LEX nr 2642798; M. Szydło [w:] M. Safjan (red.), L. Bosek (red.), Konstytucja RP, t. I, Warszawa 2016, s. 806; Wyrok TK z dnia 11 maja 1999 r.; sygnatura: K 13/98; OTK 1999, Nr 4, poz. 74.

⁶⁷ Zob. np.: M. Stahl, Dobro wspólne w prawie administracyjnym [w:] J. Boć (red.), A. Chajbowicz (red.), Nowe problemy badawcze w teorii prawa administracyjnego, Wrocław 2009.

⁶⁸ Por. szerzej: Wyrok NSA z dnia 14 grudnia 2011 r.; sygnatura: II OSK 2062/11; LEX nr 1152132; Wyrok WSA w Gliwicach z dnia 4 listopada 2011 r.; sygnatura: II SA/Gl 621/11; LEX nr 1152570.

⁶⁹ Por. szerzej: Wyrok NSA z dnia 23 kwietnia 2020 r.; sygnatura: II OSK 1917/19; LEX nr 3041318.

⁷⁰ Zob. np.: R. W. Kaszubski, A. Koniewicz, *Zasady działalności gospodarczej w świetle Konstytucji Rzeczypospolitej Polskiej*, Głosa 7/2000, s. 5; R. W. Kaszubski, J. Kołkowski, *Wolność gospodarcza w świetle Konstytucji RP*, Głosa 6/2000, s. 7; J. Grabowski, *Rola i funkcje prawa w systemie gospodarki rynkowej* [w:] *Institucje współczesnego prawa administracyjnego: księga jubileuszowa prof. zw. dra hab. Józefa Filipka*, Kraków 2001, s. 216; K. Sobczak, *Wolność gospodarcza a władza publiczna*, Przegląd Ustawodawstwa Gospodarczego 12/2000, s. 17.

zwłaszcza z art. 20 Konstytucji RP, który ustanawia fundamenty gospodarki Rzeczypospolitej Polskiej⁷¹ - społeczną gospodarkę rynkową⁷² opartą na wolności działalności gospodarczej⁷³, własności prywatnej oraz współpracy partnerów społecznych.

94. Treść prawa własności obejmuje zatem konstytucyjnie gwarantowaną wolność nabywania mienia, jego zachowania oraz swobodnego dysponowania nim. W opiniowanych przepisach ingerencja dotyczy właśnie tych podstawowych uprawnień: decyzja o uznaniu dostawcy sprzętu lub oprogramowania za tzw. dostawcę wysokiego ryzyka - decyzja podejmowana w okolicznościach całkowicie niezależnych od przedsiębiorców telekomunikacyjnych - rodzi skutki, które mogą realnie pozbawić ich zdolności wykonywania działalności gospodarczej. A skoro przedsiębiorca traci możliwość korzystania z mienia, zachowania go i dysponowania nim, to zostaje naruszona sama istota jego prawa własności.
95. Zasada, zgodnie z którą ograniczenia wolności i praw mogą być wprowadzane wyłącznie wtedy, gdy są konieczne w demokratycznym państwie, wymaga przeprowadzenia klasycznego testu proporcjonalności: należy odpowiedzieć na pytanie, czy regulacja rzeczywiście jest w stanie doprowadzić do zamierzonego celu; czy jest środkiem koniecznym - to znaczy, czy cel ten nie mógłby zostać osiągnięty przy użyciu środków mniej dotkliwych; oraz czy ciężary nakładane na obywateli pozostają w racjonalnej proporcji do przewidywanych korzyści. Dopiero pozytywna odpowiedź na wszystkie trzy pytania otwiera drogę do uznania regulacji za zgodną z Konstytucją RP.
96. Dlatego, jak wynika z orzecznictwa, ograniczenie prawa własności może zostać uznane za konstytucyjnie dopuszczalne tylko wtedy, gdy rzeczywiście służy ochronie wartości konstytucyjnych i gdy jest niezbędne. Innymi słowy - ustawodawca, sięgając po tak daleko idący środek, jak ingerencja w sferę własności prywatnej, musi wykazać, że nie istnieje alternatywa mniej uciążliwa, równie skuteczna, a bardziej przyjazna konstytucyjnym wolnościom jednostki.
97. W przypadku analizowanej regulacji warunek ten nie został spełniony. Ingerencja w prawa majątkowe przedsiębiorców telekomunikacyjnych - z powodu jej nieproporcjonalnego charakteru - wykracza poza konstytucyjnie dopuszczalne ramy. Trybunał Konstytucyjny wielokrotnie wskazywał, że przesłanka „porządku publicznego”, choć sama w sobie jest pojęciem stosunkowo szerokim i elastycznym, nie może stanowić pretekstu do ograniczeń nadmiernych. Porządek publiczny oznacza bowiem taki stan funkcjonowania wspólnoty, który umożliwia harmonijne współżycie jednostek i ochronę dóbr społecznych, w tym

⁷¹ Por. szerzej: Wyrok TK z dnia 30 stycznia 2001 r.; sygnatura: K 17/00; OTK ZU nr 1/2001, poz. 4.

⁷² Zob. np.: T. Długosz, *Spółeczna gospodarka rynkowa jako kryterium organizacji gospodarki*, Gdańskie Studia Prawnicze 2017, tom XXXVII, s. 21; A. Wałaszek-Pyziół, *Zasada proporcjonalności w orzecznictwie Trybunału Konstytucyjnego*, Przegląd Ustawodawstwa Gospodarczego 1/1995, s. 14; T. Asman, *Dopuszczalna ingerencja w wolność gospodarczą w świetle zasady proporcjonalności*, Studia i Prace Kolegium Zarządzania i Finansów Szkoły Głównej Handlowej 57/2005, s. 80-81.

⁷³ Por. szerzej: Wyrok WSA w Opolu z dnia 9 czerwca 2022 r.; sygnatura: II SA/Op 125/22; Legalis.

mienia publicznego. Ograniczenie prawa własności może być zatem uzasadnione powołaniem się na porządek publiczny, lecz tylko wówczas, gdy rzeczywiście służy ochronie tej wartości, a nie ją narusza.

98. Tymczasem w przypadku opiniowanych przepisów naruszeniu ulega fundament o wiele głębszy: zasada zaufania obywatela do państwa i stanowionego przez nie prawa. Regulacja, która nakłada na przedsiębiorcę ciężary wynikające z okoliczności absolutnie od niego niezależnych i której skutki mogą prowadzić do pozbawienia go możliwości kontynuowania działalności, nie może zostać uznana ani za racjonalną, ani za proporcjonalną, ani tym bardziej za zgodną z zasadą państwa prawnego.
99. Trybunał Konstytucyjny zawsze zaznaczał, że ocena merytorycznej trafności przyjmowanych rozwiązań należy do ustawodawcy. Trybunał nie ingeruje w polityczną czy ekonomiczną słuszość decyzji ustawodawcy. Jednak gdy ustawodawca wykracza poza konstytucyjne granice swojej swobody i narusza określoną wartość konstytucyjną - wówczas otwiera się przestrzeń dla kontroli konstytucyjnej. I właśnie w tym punkcie, w świetle przedstawionych argumentów, opinia o niekonstytucyjności analizowanych przepisów Projektu Ustawy znajduje pełne uzasadnienie.
100. W dotychczasowym dorobku orzecznictwym podkreślano wielokrotnie, że ustawodawca - w granicach wytyczonych przez Konstytucję RP - posiada prawo do kształtowania porządku prawnego również w sposób mniej korzystny dla obywateli. Może tego dokonać, o ile żadna z przyjętych regulacji nie narusza norm nadrzędnych⁷⁴. W odniesieniu do opiniowanych przepisów Projektu Ustawy naruszenie to jest widoczne. Wprowadzają one bowiem takie ograniczenia prawa własności, które wymykają się poza ramy, jakie dla ustawodawcy określa art. 64 Konstytucji RP w związku z art. 31 ust. 3 Konstytucji RP⁷⁵. Skutkiem jest nie tylko naruszenie gwarancji konstytucyjnych, lecz również to, że cele, które ustawodawca zamierzał osiągnąć, nie mogą zostać zrealizowane za pomocą środków zgodnych z Konstytucją RP. Trafność tych celów - z punktu widzenia polityki państwa - pozostaje tu bez znaczenia; istotny jest sposób ich realizacji, a ten, w świetle konstytucyjnych standardów, okazuje się niedopuszczalny⁷⁶.
101. Na tym jednak nie kończą się uchybienia. Przepisy wprowadzające szerokie wyłączenia stosowania podstawowych instytucji k.p.a. w sprawach dotyczących uznania danego podmiotu za dostawcę wysokiego ryzyka - w szczególności wyłączenia dotyczące

⁷⁴ Por. szerzej: Wyrok NSA z dnia 23 kwietnia 2020 r.; sygnatura: II OSK 1917/19; LEX nr 3041318.

⁷⁵ Por. szerzej: Wyrok NSA z dnia 14 grudnia 2011 r.; sygnatura: II OSK 2062/11; LEX nr 1152132; Wyrok WSA w Gliwicach z dnia 4 listopada 2011 r.; sygnatura: II SA/Gl 621/11; LEX nr 1152570.

⁷⁶ Por. szerzej: Postanowienie NSA z dnia 6 czerwca 2019 r.; sygnatura: II OSK 166/18; Legalis; Wyrok NSA z dnia 5 czerwca 2019 r.; sygnatura: II OSK 598/19; Wyrok NSA z dnia 6 marca 2019 r.; sygnatura: II OSK 1023/17; Legalis; Wyrok NSA z dnia 28 lutego 2019 r.; sygnatura: I OSK 874/17; Legalis; por. także: wyrok NSA z dnia 11 stycznia 2017 r.; sygnatura: II OSK 932/15; Legalis; Wyrok NSA z dnia 01 czerwca 2012 r.; sygnatura: II OSK 844/12; Legalis; Wyrok TK z dnia 23 października 2012 r.; sygnatura: SK 11/12; Legalis; Wyrok NSA z dnia 12 stycznia 2016 r.; sygnatura: II OSK 1132/14; Legalis; Wyrok NSA z dnia 10 października 2017 r.; sygnatura: II OSK 265/16; Legalis.

pojęcia strony, praw organizacji społecznych, obowiązku osobistego stawiennictwa, metryki sprawy czy praw strony - uderzają w samo serce gwarancji proceduralnych, które konstytuują demokratyczne państwo prawne.

102. Bo w demokratycznym państwie prawnym ograniczenie praw strony w postępowaniu nie jest drobną modyfikacją proceduralną - jest ograniczeniem prawa do prawa, fundamentu, na którym opiera się cała konstrukcja ochrony jednostki przed arbitralnością władzy publicznej.
103. W tym kontekście projektowane rozwiązania jawią się jako sprzeczne z konstytucyjną zasadą rzetelności i sprawności działania instytucji publicznych, wyrażoną w preambule Konstytucji RP. Trybunał Konstytucyjny wielokrotnie wskazywał, że zasada ta nie ma charakteru jedynie deklaratywnego⁷⁷. Przeciwnie - stanowi wzorzec kontroli norm, szczególnie wtedy, gdy w grę wchodzi gwarancje proceduralne podmiotów występujących przed organami władzy publicznej⁷⁸. Trybunał Konstytucyjny stosował ją zarówno wprost, jak i jako wzmocnienie argumentacji dotyczącej innych wzorców konstytucyjnych, podkreślając, że każdy ustawowy mechanizm, który z góry zakłada lub dopuszcza niemożność rzetelnego działania instytucji publicznej, staje się z tej przyczyny niezgodny z Konstytucją RP. Ustawodawca, uchwalając opiniowane przepisy, naruszył tę zasadę, tworząc konstrukcję postępowania obarczoną ryzykiem arbitralności oraz faktycznego wyłączenia ochrony prawnej przedsiębiorców telekomunikacyjnych. W ten sposób nie tylko naruszono ich konstytucyjne prawa proceduralne, ale również wprowadzono rozwiązania, które uniemożliwiają, w sensie strukturalnym, rzetelne i sprawne działanie właściwego organu.
104. Trybunał już wcześniej zauważał, że instytucja publiczna zaprojektowana w sposób uniemożliwiający jej prawidłowe funkcjonowanie staje się naruszeniem zasad państwa prawnego. W jednym z orzeczeń wyraźnie podkreślono, że dotyczy to zwłaszcza instytucji, których zadaniem jest ochrona praw konstytucyjnych lub zapewnienie porządku i bezpieczeństwa publicznego. Skoro Konstytucja RP tworzy ramy działania tych instytucji, ustawodawca nie może osłabiać ich rzetelności poprzez arbitralne modyfikacje proceduralne.
105. Stąd wywiedziono również ogólną regułę: rzetelność i sprawność działania instytucji publicznych, szczególnie tych stojących na straży praw i wolności jednostki, jest wartością konstytucyjną⁷⁹. Wynika to wprost z preambuły, w której dwa cele stoją obok siebie - zagwarantowanie praw obywatelskich oraz zapewnienie rzetelności działania

⁷⁷ Por. np.: Wyrok TK z 3.11.2006 r., K 31/06, OTK-A 2006, nr 10, poz. 147.

⁷⁸ Por. np.: Wyrok TK z 7.01.2004 r., K 14/03, OTK-A 2004, nr 1, poz. 1.

⁷⁹ Por. szerzej np.: A.M. Wiltos, prawo jednostki do rzetelnego i sprawnego działania instytucji publicznych, Warszawa 2024, Rozprawa doktorska napisanej pod kierunkiem prof. dra hab. Janusza Trzeźnińskiego, na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego; por. także: Wyrok TK z 11.08.2016 r., K 39/16, OTK-A 2016, nr 71.

instytucji publicznych⁸⁰. Oba są nierozzerwalne. Normy, które podważają rzetelność instytucji, podważają tym samym prawa obywateli. A skoro tak, to przepisy, które nie sprzyjają działaniu instytucji w sposób przejrzysty i zgodny z zasadą dobra wspólnego, muszą zostać uznane za niezgodne z Konstytucją RP.

106. Projektowana regulacja zawarta w art. 67e ust. 2 Projekcie Ustawy przewiduje, że odpis sentencji wyroku sądu administracyjnego, wydanego w następstwie kontroli decyzji o uznaniu danego podmiotu za dostawcę wysokiego ryzyka, doręcza się stronie skarżącej wraz z tą częścią uzasadnienia, która nie zawiera informacji niejawnych. Na pierwszy rzut oka rozwiązanie to może sprawiać wrażenie naturalnego - wszak sprawa dotyczy obszaru bezpieczeństwa państwa, gdzie wrażliwość informacji bywa szczególna. Jednak analiza konstytucyjna nie pozwala przejść obok tego przepisu obojętnie.
107. W art. 45 ust. 2 Konstytucji RP dopuszcza bowiem wyłączenie jawności rozprawy, a więc określonego etapu procedowania, motywowanego szczególnymi okolicznościami: ochroną moralności, bezpieczeństwa państwa, porządku publicznego, a także ochroną życia prywatnego stron⁸¹. Nie przewiduje natomiast możliwości wyłączenia jawności uzasadnienia wyroku, które stanowi integralną część samego aktu orzeczniczego. Ustawodawca konstytucyjny sformułował tu zasadę prostą i stanowczą: wyrok ogłasza się publicznie - a jego uzasadnienie jest częścią tego wyroku, a nie dodatkiem, który można dowolnie modyfikować lub fragmentaryzować.
108. Uzasadnienie pełni rolę nie tylko sprawozdawczą, ale przede wszystkim gwarancyjną: pozwala stronie, jak i opinii publicznej, zrozumieć tok rozumowania sądu, kontrolować jego rzetelność, a w konsekwencji - stanowi fundament zaufania do wymiaru sprawiedliwości⁸². Dlatego też ograniczenie jawności uzasadnienia, nawet motywowane ochroną informacji niejawnych, wymaga szczególnej ostrożności i nie może naruszać konstytucyjnych standardów transparentności wymiaru sprawiedliwości⁸³. Projektowane

⁸⁰ Por. szerzej: Wyrok TK z 22.10.2020 r., K 1/20, OTK-A 2021, nr 1; Wyrok TK z 21.09.2011 r., SK 6/10, OTK-A 2011, nr 7, poz. 73; Wyrok TK z 29.09.2008 r., SK 52/05, OTK-A 2008, nr 7, poz. 125; Postanowienie TK z 15.12.2022 r., K 49/15, OTK-A 2023, nr 12.

⁸¹ Por. szerzej np.: P. Tuleja [w:] P. Czarny, M. Florczak-Wątor, B. Naleziński, P. Radziejewicz, P. Tuleja, Konstytucja Rzeczypospolitej Polskiej. Komentarz, wyd. II, Warszawa 2023, art. 45; P. Sarnecki [w:] Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II, wyd. II, red. L. Garlicki, M. Zubik, Warszawa 2016, art. 45; A. Ławniczak [w:] Konstytucja Rzeczypospolitej Polskiej. Komentarz, red. M. Haczkowska, Warszawa 2014, art. 45.

⁸² Por. np.: Wyrok TK z 16.12.2008 r., P 17/07, Dz.U. nr 228, poz. 1524; por. także szerzej: M. Żak, Prawo do sądu jako element zasady dobrego rządzenia w świetle orzecznictwa z zakresu praw człowieka, Palestra 2020, nr 2.

⁸³ Zob. np. Wyrok TK z 30.10.2012 r., SK 8/12, OTK-A ZU 2012/9, poz. 111. W uzasadnieniu przedmiotowego wyroku TK wskazał, że: *ustawodawca dysponuje szerokim zakresem swobody w kształtowaniu procedur sądowych, w tym w stanowieniu wymogów formalnych w celu usprawnienia postępowania, ale w granicach, w jakich nie niweczy to celu danego postępowania.*

rozwiązanie, poprzez swój konstrukcyjny automatyzm i szerokość zastosowania, budzi poważne wątpliwości co do jego zgodności z art. 45 Konstytucji RP⁸⁴.

109. Jeszcze poważniejsze problemy niesie ze sobą art. 67g ust. 2 Projektu Ustawy, dotyczący tzw. polecenia zabezpieczającego wydawanego przez ministra właściwego do spraw informatyzacji. Zgodnie z projektowaną regulacją przedstawioną w Projekcie Ustawy polecenie to jest kierowane do nieokreślonego kręgu podmiotów kluczowych i podmiotów ważnych - a więc do szerokiego spektrum aktorów funkcjonujących w strategicznych sektorach państwa.
110. I tu ujawnia się fundamentalny problem o charakterze ustrojowym. Konstytucja RP w art. 87 ust. 1 enumeratywnie wskazuje źródła prawa powszechnie obowiązującego. W aktualnym stanie prawnym ich zamknięty katalog⁸⁵ zawiera przepis z art. 87 Konstytucji RP⁸⁶ (jest to: Konstytucja RP⁸⁷, ustawy⁸⁸, ratyfikowane umowy międzynarodowe oraz rozporządzenia, a także na obszarze działania organów, które je ustanowiły, akty prawa miejscowego)⁸⁹. Polecenia ministra się w tym katalogu nie mieszczą. Nie są rozporządzeniami, których wydawanie wymaga istnienia ustawowej delegacji oraz zbioru gwarancji zapewniających ich legalność, kontrolowalność i generalny charakter. Polecenie - nawet jeśli nosi znamiona władczości - nie jest aktem normatywnym powszechnie obowiązującym.
111. Co więcej, adresatami poleceń ministra mogą być wyłącznie jednostki organizacyjnie mu podległe. Tymczasem podmioty wymienione w art. 67g ust. 2 Projektu Ustawy nie podlegają ministrowi właściwemu do spraw informatyzacji ani w sensie zwierzchnictwa organizacyjnego, ani w sensie nadzoru administracyjnego. Oznacza to, że nawet gdyby polecenie ministra zostało sformułowane w formie zarządzenia, nie mogłoby

⁸⁴ Zob. np.: M. Kryszkiewicz, Bez uzasadnienia orzeczenia, bez prawa do obrony, *Gazeta Prawna*, 1 lutego 2022, 06:00, dostęp: <https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/8346496,rpo-uzasadnienie-orzeczenia-prawo-do-obrony-gwarancje-procesowe.html> (data dostępu: 02.12.2025 r.).

⁸⁵ O zamkniętym charakterze katalogu źródeł prawa powszechnie obowiązującego: Wyrok TK z 20 października 1998 r., K 7/98, OTK 1998, Nr 6, poz. 96; Wyrok NSA z 13 stycznia 2011 r., sygnatura: I OSK 1257/10, LEX nr 951947; Wyrok WSA w Warszawie z dnia 10 kwietnia 2013 r., sygnatura: II SA/Wa 1820/12, LEX nr 1616967; Wyrok WSA w Warszawie z dnia 16 listopada 2012 r., sygnatura: II SA/Wa 1156/12, LEX nr 1249048; wyrok WSA w Warszawie z dnia 22 listopada 2012 r., sygnatura: II SA/Wa 1261/12, LEX nr 1249066; K. Działocha, *Zamknięty system źródeł prawa powszechnie obowiązującego w Konstytucji i w praktyce* [w:] *Konstytucyjny system źródeł prawa w praktyce*, (red.) A. Szmyt, Warszawa 2005, s. 12.

⁸⁶ Por. także: Wyrok NSA z dnia 13.11.2012 r., sygnatura: II GSK 1727/11; Legalis.

⁸⁷ Zob.: L. Garlicki, *Konstytucyjne źródła prawa administracyjnego* [w:] *System Prawa Administracyjnego*. Tom 2, *Konstytucyjne podstawy funkcjonowania administracji publicznej*, (red.) R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2012, s. 87-88.

⁸⁸ Por.: L. Garlicki, M. Zubik, *Ustawa w systemie źródeł prawa* [w:] *Konstytucyjny system źródeł prawa w praktyce*, (red.) A. Szmyt, Warszawa 2005, s. 56 i n.

⁸⁹ Tak: A. Krawczyk [w:] W. Chróścielewski (red.), Z. Kmiecik (red.), *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2018, komentarz do art. 107 k.p.a.; por. także: P. Majczak, *Dyrektywa jako podstawa prawna decyzji administracyjnej*, *Acta Universitatis Wratislaviensis* No 3771, *Prawo CCCXXII*, Wrocław 2017, s. 46; P. Majczak, *Podstawa prawna decyzji administracyjnej*, *Ius Novum* 2016, nr 4, s. 377-379

wiązać tych podmiotów - a tym bardziej nie może ich wiązać akt, który nie posiada statusu aktu normatywnego ani aktu wewnętrznego w rozumieniu Konstytucji RP.

112. W efekcie projektowane i ujęte w treści Projektu Ustawy rozwiązanie tworzy konstrukcję, która nie mieści się w konstytucyjnym systemie źródeł prawa, a jednocześnie nakłada na podmioty o kluczowym znaczeniu dla funkcjonowania państwa obowiązki, które nie mają umocowania w obowiązującym porządku prawnym. To zaś prowadzi do wniosku, że regulacja ta narusza nie tylko zasady państwa prawnego, lecz również zasadę legalizmu, zgodnie z którą organy władzy publicznej działają na podstawie i w granicach prawa.

III.5. Ingerencja w działalność gospodarczą poprzez możliwość nakazania wstrzymania działalności lub cofnięcia koncesji.

113. Projekt Ustawy nowelizującej ustawę o krajowym systemie cyberbezpieczeństwa, poprzez rozszerzenie obowiązków na osiemnaście sektorów gospodarki oraz wprowadzenie mechanizmu zawieszenia lub cofnięcia koncesji bądź zezwolenia na prowadzenie działalności, stanowi szczególnie daleko idącą ingerencję w konstytucyjnie chronioną swobodę działalności gospodarczej oraz w prawo własności. Rozwiązania te wymagają oceny zarówno pod kątem zgodności z prawem Unii Europejskiej, jak i ze standardami krajowymi, w tym zasadą proporcjonalności oraz zasadą pewności prawa.
114. Zgodnie z art. 49 Karty Praw Podstawowych oraz art. 16 i art. 17 Karty Praw Podstawowych⁹⁰, prawo do prowadzenia działalności gospodarczej i prawo własności mogą być ograniczane jedynie wtedy, gdy jest to konieczne, proporcjonalne i wynika z rzeczywistego interesu publicznego, w sposób nienaruszający istoty tych praw. Jednocześnie Dyrektywa NIS2, którą Projekt Ustawy ma implementować, nie przewiduje mechanizmu automatycznego zawieszenia działalności reglamentowanej ani cofnięcia koncesji w następstwie naruszeń obowiązków cyberbezpieczeństwa. System sankcyjny przewidziany w postanowieniach Dyrektywy NIS2 opiera się na środkach dostosowanych do charakteru naruszenia i ryzyka, a nie na środkach o charakterze *quasi*-represyjnym mogących prowadzić do natychmiastowego paraliżu działalności gospodarczej⁹¹.
115. Analiza projektowanego art. 53e Projektu Ustawy wskazuje, że procedura ingerencji w działalność gospodarczą ma charakter niemal automatyczny. Organ właściwy ds. cyberbezpieczeństwa, będący w zależności od sektora m.in. ministrem właściwym do spraw energii czy cyfryzacji, uzyskuje możliwość wystąpienia z wnioskiem o zawieszenie koncesji lub cofnięcie zezwolenia bez uprzedniego ostrzeżenia, zaś organ koncesyjny lub

⁹⁰ Por. szerzej: M. Górski, Przepisy o cyberbezpieczeństwie budzą wiele wątpliwości, <https://www.rp.pl/polityka/art41459811-prof-marcin-gorski-przepisy-o-cyberbezpieczenstwie-budza-wiele-watpliwosci> (data dostępu: 02.12.2025 r.).

⁹¹ Por. szerzej: E. Rutkowska, *Łatwo będzie stracić koncesję. Wszystko ze względów cyberbezpieczeństwa*, Dziennik Gazeta Prawna, (data dostępu: 8 grudnia 2024, 20:51).

sąd administracyjny związany jest oceną zawartą we wniosku, o ile *informacje w nim zawarte nie budzą wątpliwości*. Konstrukcja ta *de facto* eliminuje możliwość merytorycznej kontroli proporcjonalności środka przez organ koncesyjny, redukując jego rolę do formalnego potwierdzenia danych przedstawionych przez organ cyberbezpieczeństwa.

116. W praktyce oznacza to, że jednostronna ocena organu cyberbezpieczeństwa może prowadzić do natychmiastowego wstrzymania działalności przedsiębiorcy funkcjonującego na rynku reglamentowanym - w sektorach takich jak wytwarzanie i przesyłanie energii, górnictwo, gospodarka odpadami, transport lotniczy czy działalność farmaceutyczna. Skutki takiego środka są daleko poważniejsze niż typowe sankcje administracyjne przewidziane w Dyrektywie NIS2, ponieważ ingerują bezpośrednio w możliwość prowadzenia działalności i generowania przychodów, prowadząc potencjalnie do utraty klientów, pogorszenia płynności finansowej i nieodwracalnych szkód gospodarczych⁹².
117. Zwrócić należy uwagę, że projekt nie przewiduje obowiązku analizy krytyczności zasobów, stopnia ryzyka, skali naruszenia ani możliwości zastosowania środków naprawczych przed sięgnięciem po najbardziej dotkliwy instrument - zawieszenie lub cofnięcie koncesji. Tymczasem Dyrektywa NIS2 jednoznacznie wymaga, aby środki przyjmowane przez państwa członkowskie były adekwatne oraz proporcjonalne do ryzyka dla usług kluczowych, a ich stosowanie poprzedzone było oceną faktycznych zagrożeń i możliwości zapobieżenia incydentom. Automatyzm przewidziany w projekcie pozostaje z tym standardem w sprzeczności, powodując, że ingerencja w działalność przedsiębiorstwa jest możliwa nawet w sytuacji braku związku pomiędzy naruszeniem a realnym zagrożeniem dla bezpieczeństwa państwa lub obywateli.
118. Dodatkowym problemem jest przewidziana w Projekcie Ustawy konstrukcja proceduralna, która ogranicza rolę organu koncesyjnego do rozpoznania wniosku bez pełnej swobody oceny okoliczności sprawy. Wyłączenie realnej kontroli merytorycznej oznacza, że organ odpowiada za decyzję ingerującą w najbardziej chronione sfery aktywności gospodarczej, nie mając faktycznej możliwości weryfikacji, czy naruszenie oraz jego skutki uzasadniają zastosowanie środka prowadzącego w praktyce do eliminacji przedsiębiorcy z rynku. Takie rozwiązanie narusza nie tylko zasadę proporcjonalności, ale również zasadę legalizmu i pewności prawa⁹³, które wymagają, aby sankcje były stosowane wyłącznie po rzetelnej i obiektywnej analizie.

⁹² Zob. np.: B. Adamiak, *Prawo do sądu jako gwarancja wolności gospodarczej* [w:] *Granice wolności gospodarczej w systemie społecznej gospodarki rynkowej. Księga jubileuszowa z okazji 40-lecia pracy naukowej prof. dr hab. Jana Grabowskiego*, Katowice 2004.

⁹³ Por. np.: M. Baran, *Zasada pewności prawa a zasada legalizmu unijnego – uwagi na tle orzecznictwa TS*, Europejski Przegląd Sądowy 5/2011; A. Kluczevska-Rupka, *Zasada pewności prawa w działaniu administracji Unii Europejskiej oraz jako zasada ogólna prawa Unii Europejskiej*, *Studia Prawa Publicznego* 1(5)/2014; por. także: Wyrok WSA w Gliwicach z dnia 7 sierpnia 2014 r.; sygnatura: IV SAB/GI 89/14; LEX nr 1513998.

119. Na szczególne podkreślenie zasługuje również fakt, że zawieszenie koncesji, cofnięcie zezwolenia bądź wstrzymanie działalności nie zostały w Dyrektywie NIS2 przewidziane jako środki podstawowe, lecz - co wynika z jej konstrukcji - mogą być stosowane jedynie w ramach krajowych reżimów koncesyjnych, z poszanowaniem krajowego porządku prawnego i przy zachowaniu kontroli sądowej obejmującej ocenę proporcjonalności. Projektowane rozwiązania idą dalej niż wymogi dyrektywy, tworząc instrument o mocy silniejszej niż znane dotychczas narzędzia nadzorcze w sektorach reglamentowanych, a jednocześnie eliminując proceduralne gwarancje⁹⁴ ograniczające ryzyko nadużyć.
120. W konsekwencji implementacja przyjęta w Projekcie Ustawy przyznaje organowi cyberbezpieczeństwa rolę super-regulatora, zdolnego oddziaływać na decyzje organów koncesyjnych w sposób determinujący ich treść. Może to prowadzić do powstania systemowego ryzyka paraliżu działalności gospodarczej, zwłaszcza w sektorach o znaczeniu strukturalnym dla funkcjonowania państwa i gospodarki, w których nieprzerwane wykonywanie działalności stanowi element bezpieczeństwa publicznego.
121. Choć projektodawca w treści Projektu Ustawy wskazuje, że ww. środki mają być stosowane jako „ostateczne”, to jednocześnie treści wprowadzanej regulacji prawnej nie przewidziano jednoznacznych mechanizmów gwarancyjnych, wymogu oceny adekwatności środka w stosunku do naruszenia, co budzi bardzo istotne i uzasadnione obawy o adekwatne zabezpieczenie ochrony sfery interesów i praw podmiotów wobec których możliwe będzie stosowanie ww. środków. Dodatkowo, zwrócić należy także uwagę na aspekt przewagi elementu automatyzmu przewidziany w Projekcie Ustawy w zakresie stosowania ww. środków, co powoduje, że zapewnienia te nie znajdują odzwierciedlenia w treści projektowanej regulacji.
122. Rozwiązanie to zatem nie realizuje wymogów Dyrektywy NIS2 i nie zapewnia zgodności z zasadami prawa UE ani z konstytucyjnymi standardami ograniczania praw podmiotowych, wobec czego apeluję aby prawodawca pochylił się nad tymi rozwiązaniami oraz dokonał ich adekwatnej modyfikacji.

III.6. Porównanie implementacji w kontekście zakresu i skali wprowadzanych obowiązków na poziomie państwa członkowskich UE.

123. Warto także zauważyć, iż analizowany Projekt Ustawy i projektowana przez polskiego prawodawcę implementacja Dyrektywy NIS2 ma charakter najszerzej i najbardziej restrykcyjnej regulacji w Europie. Polska nowelizacja ustawy o krajowym

⁹⁴ Por. np.: B. Adamiak, *Prawo do sądu jako gwarancja wolności gospodarczej* [w:] *Granice wolności gospodarczej w systemie społecznej gospodarki rynkowej. Księga jubileuszowa z okazji 40-lecia pracy naukowej prof. dr hab. Jana Grabowskiego*, Katowice 2004, s. 13–20; P. Przybysz, *Prawo do sądu w sprawach administracyjnych* [w:] *Prawo administracyjne w okresie transformacji ustrojowej*, red. E. Knosala, A. Matan, G. Łaszczyca, Kraków 1999, s. 347–348.

systemie cyberbezpieczeństwa nie tylko przewiduje największy katalog obowiązków, lecz dodatkowo wprowadza mechanizmy, które znacząco wykraczają poza zakres unijnego prawodawstwa, zarówno w treści, jak i negatywnych skutkach dla rynku wewnętrznego polegającego na fragmentacji rynku wewnętrznego, zagrożenia dla jego jednolitości i dla jednolitego stosowania prawa Unii Europejskiej - w wyniku zróżnicowania poziomu obciążeń regulacyjnych i zakresu obowiązków nakładanych na adresatów regulacji w poszczególnych państwach członkowskich - mimo że regulacje te mają implementować ten sam „wzorzec unijny” i realizować te same cele.

124. Zwrócić także należy uwagę na fakt, iż Polska jawi się jako jedyny kraj planujący równoczesne, w jednej ustawie, wdrożenie Dyrektywy NIS2 i zaleceń 5G Toolbox, przy czym ograniczenia wobec dostawców wysokiego ryzyka mają objąć wszystkie 18 sektorów wskazanych w Dyrektywie NIS2⁹⁵. Konstrukcja ta obejmuje co najmniej 38 tysięcy podmiotów⁹⁶, wykraczając poza standard praktyk państw członkowskich i nadając zaleceniom Toolbox *de facto* charakter powszechnego punktu odniesienia dla całej gospodarki, a nie wyłącznie dla telekomunikacji. Jednocześnie przewiduje się możliwość usuwania już użytkowanego sprzętu, bez środków naprawczych, oraz obowiązek wycofywania produktów i usług ICT od dostawców wysokiego ryzyka bez uprzedniej analizy krytyczności zasobów - co na tle UE stanowi podejście wyjątkowo szerokie i restrykcyjne⁹⁷.
125. Kontekst prawny i regulacyjny wskazuje, że NIS2 ustanawia ogólne, bardziej rygorystyczne ramy cyberbezpieczeństwa, a 5G Toolbox pozostaje zestawem zaleceń - niewiążącym, choć silnie promowanym - do ochrony sieci 5G. W Polsce przyjęto model jednoczesnego wdrożenia obu reżimów w jednej ustawie i rozszerzono zastosowanie rozwiązań 5G Toolbox na wszystkie sektory kluczowe i ważne, co wyraźnie odbiega od praktyki większości państw członkowskich, które ograniczają te środki do sektora telekomunikacyjnego i sieci 5G⁹⁸.
126. W efekcie tak zaprojektowanego wdrożenia uwidaczniają się trzy, kluczowe wymiary skali istotnie odróżniające nadmiarowy sposób implementacji przepisów

⁹⁵ Por. np.: <https://www.pwc.pl/pl/uslugi/nis2-nowe-wymogi-dotyczace-cyberbezpieczenstwa.html> (data dostępu: 02.12.2025 r.).

⁹⁶ Zob.: Raport EY pt. „Regulacje NIS2 i 5G Toolbox w Polsce. Analiza wdrożenia i porównanie z państwami UE”, dostęp: https://www.ey.com/pl_pl/insights/law/raport-ey-regulacje-nis2-i-5g-toolbox-w-polsce-analiza-wdrozenia-i-porownanie-z-panstwami-ue (data dostępu: 02.12.2025 r.), s. 6; ; por. analogicznie: Certyfikacja zamiast blokowania – to odpowiedź na zmianę prawa, dostęp: <https://cyfrowa-gospodarka.gazetaprawna.pl/biznes/9506680.certyfikacja-zamiast-blokowania-to-odpowiedz-na-zmiane-prawa.html> (data dostępu: 02.12.2025 r.).

⁹⁷ Tak: Raport EY pt. „Regulacje NIS2 i 5G Toolbox w Polsce. Analiza wdrożenia i porównanie z państwami UE”, dostęp: https://www.ey.com/pl_pl/insights/law/raport-ey-regulacje-nis2-i-5g-toolbox-w-polsce-analiza-wdrozenia-i-porownanie-z-panstwami-ue (data dostępu: 02.12.2025 r.), s. 3.

⁹⁸ Wątek ten został szczegółowo przedstawiony w treści Raportu EY pt. „Regulacje NIS2 i 5G Toolbox w Polsce. Analiza wdrożenia i porównanie z państwami UE”, dostęp: https://www.ey.com/pl_pl/insights/law/raport-ey-regulacje-nis2-i-5g-toolbox-w-polsce-analiza-wdrozenia-i-porownanie-z-panstwami-ue (data dostępu: 02.12.2025 r.), s. 10-37.

Dyrektywy NIS2 w Polsce w stosunku do pozostałych państwa członkowskich Unii Europejskiej. Zwrócić bowiem należy uwagę na różnice objawiające się w zasięgu sektorowym - w Polsce dochodzi do objęcia wszystkich sektorów NIS2, a nie tylko telekomunikacji.

127. Przedmiotowa różnica uwidacznia się także w kontekście zakresu podmiotowego, gdzie w Polsce nowe, nadmiarowe rozwiązania ujęte w treści Projektu Ustawy znajdują zastosowanie do co najmniej 38-40 tysięcy adresatów⁹⁹, podczas gdy w innych państwach członkowskich odsetek adresatów jest bardziej ograniczony liczebnie¹⁰⁰. Dostrzec także należy, że polska implementację Dyrektywy NIS2 w stosunku do implementacji przyjmowanych w innych państwach członkowskich Unii Europejskiej odróżnia także charakter obowiązków - odejście od rekomendowanego w Toolbox modelu stopniowego, ryzyko-bazowego wdrażania ograniczeń, w kierunku wykluczeń „z góry”. Jednocześnie, na tle unijnej kategoryzacji elementów krytycznych 5G, Toolbox nie uznaje standardowo radiowej sieci dostępowej (RAN) za element krytyczny, wskazując, że jej znaczenie może rosnać dopiero w architekturze *stand-alone* i zależnie od faktycznej roli funkcji sieciowych - co uwypukla różnicę względem szerokiej klasyfikacji przyjmowanej w polskim Projekcie Ustawy w stosunku do innych implementacji przepisów Dyrektywy NIS2.
128. Raz jeszcze w tym miejscu stanowczo wskażę, iż Dyrektywa NIS2 ma charakter dyrektywy minimalnej harmonizacji, co oznacza, że państwo członkowskie Unii Europejskiej może wprowadzać dalej idące środki, o ile spełnione zostaną kumulatywnie następujące wymogi, tj.: (i) nie naruszają innych wiążących aktów prawa unijnego; (ii) pozostają spójne z krajowym porządkiem konstytucyjnym; (iii) spełniają wymogi proporcjonalności i subsydiarności; jak również (iv) nie naruszają swobód rynku wewnętrznego, w szczególności swobody przedsiębiorczości oraz swobody przepływu towarów. Przypomnieć w tym miejscu należy, że warunki te nie zostały spełnione przez polski Projekt Ustawy, który tworzy szereg regulacji o charakterze nadmiernym¹⁰¹, w tym rozszerza zakres Dyrektywy NIS2 na obszary oraz procedury nieprzewidziane w prawie unijnym.
129. W powyższym kontekście za jeden z najbardziej problematycznych elementów należy uznać rozszerzenie polskiej implementacji Dyrektywy NIS2 o zalecenia 5G

⁹⁹ Tak: Raport EY pt. „Regulacje NIS2 i 5G Toolbox w Polsce. Analiza wdrożenia i porównanie z państwami UE”, dostęp: https://www.ey.com/pl_pl/insights/law/raport-ey-regulacje-nis2-i-5g-toolbox-w-polsce-analiza-wdrozenia-i-porownanie-z-panstwami-ue (data dostępu: 02.12.2025 r.), s. 6; por. także: Certyfikacja zamiast blokowania – to odpowiedź na zmianę prawa, dostęp: <https://cyfrowa-gospodarka.gazetaprawna.pl/biznes/9506680,certyfikacja-zamiast-blokowania-to-odpowiedz-na-zmiane-prawa.html> (data dostępu: 02.12.2025 r.).

¹⁰⁰ W Niemczech liczba podmiotów zobowiązanych do stosowania nowych regulacji szacowana jest na poziomie 35 tys. podmiotów, w Hiszpanii 25 tys., we Francji 15 tys.; zob.: Certyfikacja zamiast blokowania – to odpowiedź na zmianę prawa, dostęp: <https://cyfrowa-gospodarka.gazetaprawna.pl/biznes/9506680,certyfikacja-zamiast-blokowania-to-odpowiedz-na-zmiane-prawa.html> (data dostępu: 02.12.2025 r.).

¹⁰¹ Zob. szerzej: T. Siemiątkowski, Szkodliwa nadregulacja w sprawie cyberbezpieczeństwa, dostęp: <https://www.rp.pl/opinie-prawne/art41473571-prof-tomasz-siemiatkowski-szkodliwa-nadregulacja-w-sprawie-cyberbezpieczenstwa> (data dostępu: 02.12.2025 r.).

Toolbox. Dokument ten, mający charakter *soft law*, został przygotowany wyłącznie z myślą o bezpieczeństwie mobilnych sieci telekomunikacyjnych, w szczególności o elementach sieci 5G posiadających znaczenie krytyczne. Zgodnie z założeniami UE, zalecenia Toolbox miały umożliwiać państwom członkowskim ocenę ryzyka w zakresie infrastruktury telekomunikacyjnej, przy jednoczesnym zachowaniu zasady proporcjonalności oraz poszanowania specyfiki krajowych systemów. Tymczasem Projekt Ustawy traktuje 5G Toolbox jako wiążący wzorzec regulacyjny, nadając mu w praktyce moc prawa obowiązującego, i co więcej - rozszerzając jego stosowanie nie tylko na wszystkie generacje sieci mobilnych i elementy nieposiadające charakteru krytycznego, ale również na wszystkie sektory wymienione w Dyrektywie NIS2.

130. W konsekwencji polskie podejście wprowadza najszerszą w Unii Europejskiej definicję infrastruktury krytycznej, uznając za krytyczne wszystkie komponenty ICT, w tym komponenty pasywne, sieci 3G, 4G, 5G oraz infrastrukturę stacjonarną. Regulacje dotyczące dostawców wysokiego ryzyka obejmują pełną listę osiemnastu sektorów NIS2 – od energetyki, transportu i bankowości, przez służbę zdrowia i gospodarkę wodną, po sektor chemiczny, spożywczy, cyfrowy i jednostki administracji publicznej. Tak szerokie ujęcie nie znajduje odpowiednika w żadnym innym państwie Unii Europejskiej i stanowi jaskrawy przykład *gold-platingu*, którego skutkiem jest naruszenie zasady proporcjonalności w prawie unijnym.
131. Jednocześnie polska regulacja wprowadza obowiązek usuwania sprzętu wykorzystywanego przez podmioty kluczowe i ważne we wszystkich sektorach zobligowanych do stosowania Dyrektywy NIS2, również tam, gdzie infrastruktura ta nie ma żadnego związku z krytycznością usług w rozumieniu prawa unijnego. Wprowadzenie powszechnego zakazu nabywania i obowiązku wycofania produktów ICT od dostawców uznanych za podmioty wysokiego ryzyka prowadzi w praktyce do ograniczenia swobody przepływu towarów oraz swobody przedsiębiorczości, co narusza podstawowe zasady rynku wewnętrznego Unii Europejskiej.
132. W innych krajach Unii Europejskiej zastosowane rozwiązania są znacząco bardziej proporcjonalne, a zakres ich stosowania pozostaje ściśle związany z rekomendacjami 5G Toolbox i ograniczony do sektora telekomunikacyjnego. I tak przykładowo w Niemczech za krytyczne uznane zostały jedynie komponenty rdzeniowej sieci 5G oraz wybrane funkcje zarządzania siecią radiową, nie obejmując regulacją pozostałych elementów RAN ani infrastruktury pasywnej. W Hiszpani natomiast ograniczono stosowanie środków do wybranych obszarów geograficznych uznanych za krytyczne, nakładając równocześnie obowiązek dywersyfikacji dostawców. Analogicznie, Irlandia dopuściła wycofywanie

niektórych krytycznych komponentów, ale uznaje, że elementy RAN nie mają charakteru krytycznego i nie podlegają obowiązkowemu wykluczeniu¹⁰².

133. Na tym tle polska implementacja Dyrektywy NIS2 przyjęta w Projekcie Ustawy jawi się jako konstrukcja wyjątkowo szeroka, dalece wykraczająca poza ramy wynikające zarówno z dyrektywy NIS2, jak i z rekomendacji unijnych. Implementacja została przeprowadzona w sposób, który nie uwzględnia ani charakteru minimalnej harmonizacji, ani potrzeby zapewnienia adekwatności i proporcjonalności środków - co w konsekwencji może prowadzić do naruszenia prawa unijnego oraz do poważnych zakłóceń funkcjonowania rynku wewnętrznego.

Z wyrazami głębokiego szacunku

 Podpisano przez/ Signed by:
PAWEŁ
WAJDA
Data/ Date: 03.12.2025 19:02
mSzafir

Prof. dr hab. Paweł Wajda

¹⁰² Tak: Raport EY pt. „Regulacje NIS2 i 5G Toolbox w Polsce. Analiza wdrożenia i porównanie z państwami UE”, dostęp: https://www.ey.com/pl_pl/insights/law/raport-ey-regulacje-nis2-i-5g-toolbox-w-polsce-analiza-wdrozenia-i-porownanie-z-panstwami-ue (data dostępu: 02.12.2025 r.), s. 9.