

Warszawa, dnia 10 lutego 2026 r.

DKKIKE-2237

Szanowny Pan
Dr Karol Nawrocki
Prezydent Rzeczypospolitej Polskiej

Szanowny Panie Prezydencie,

w imieniu członków Krajowej Izby Komunikacji Ethernetowej (dalej: „Izba”), największej – pod względem liczby członków¹ – izby gospodarczej zrzeszającej polskich przedsiębiorców telekomunikacyjnych z segmentu mikro, małych i średnich przedsiębiorstw (dalej: „MŚP”), zwracam się do Pana Prezydenta z prośbą o rozważenie zasadności podpisania ustawy z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (dalej: „Ustawa”), szczególnie w obliczu:

1. niezgodności Ustawy z Konstytucją RP, w szczególności mechanizmu tzw. dostawcy wysokiego ryzyka (dalej: „DWR”), stwierdzonej przez 5 wybitnych znawców prawa konstytucyjnego i administracyjnego;
2. ujętej w Ustawie nadregulacji, która może doprowadzić do groźnego dla polskich przedsiębiorców arbitrażu technologicznego;
3. negatywnych skutków gospodarczych rozwiązań przyjętych w Ustawie, stanowiących przy tym bezprawie legislacyjne.

Przedsiębiorcy zrzeszeni w naszej Izbie docierają z usługami telekomunikacyjnym do ok. 4 mln gospodarstw domowych, przede wszystkim w mniejszych miejscowościach w Polsce. Od początku prac nad Ustawą jesteśmy zaniepokojeni możliwymi finansowymi skutkami regulacji, w szczególności w zakresie DWR. Konsekwencje decyzji DWR będą dla nas rażąco nieproporcjonalne: obejmują nakaz usunięcia całych kategorii sprzętu i oprogramowania przed zakończeniem ich okresu amortyzacji, bez jakiejkolwiek formy odszkodowania oraz bez rozważenia środków mniej dolegliwych. Decyzja DWR wiąże się bowiem z nakazem wycofania z użytkowania sprzętu wskazanego w takiej decyzji w ciągu 4 lub 7 lat od daty jej wydania, bez odszkodowania. Co istotne, mechanizm DWR nie służy ani zwalczaniu cyberataków, ani eliminowaniu wad sprzętu, ani reagowaniu na incydenty krytyczne, natomiast może być motywowany politycznie.

Spis treści

1. Mechanizm tzw. dostawcy wysokiego ryzyka niezgodny z Konstytucją RP	2
1.1. Opis mechanizmu tzw. dostawcy wysokiego ryzyka	2
1.2. Wyłączenie bez odszkodowania (art. 21 ust. 2 i art. 64 ust. 3 Konstytucji RP)	2
1.3. Naruszenie zasad społecznej gospodarki rynkowej i swobody działalności gospodarczej (art. 20 i art. 22 Konstytucji RP)	4
1.4. Naruszenie zasady proporcjonalności (art. 2 i art. 31 ust. 3 Konstytucji RP)	4
1.5. Fikcyjne prawo do obrony (naruszenie art. 32 ust. 1, art. 45 ust. 1, art. 77 ust. 2 i art. 78 Konstytucji RP) ..	5
2. Pozostałe rozwiązania niezgodne z Konstytucją RP	6
2.1. Polecenie zabezpieczające (art. 87 ust. 1 Konstytucji RP – źródła prawa)	6
2.2. Metodyki nadzoru – opinia Biura Legislacyjnego Senatu RP (art. 2, 87 i 92 ust. 1 Konstytucji RP)	6
3. Bezprawie legislacyjne: ryzyko wielomiliardowych roszczeń odszkodowawczych wobec Skarbu Państwa	7
4. Nadregulacja i arbitraż technologiczny	7
5. USA? Chiny? A może jednak Polska	8
5.1. DWR to nie jest eliminacja wad w sprzęcie ICT i oprogramowaniu	8
5.2. Polscy przedsiębiorcy MŚP a bezpieczeństwo narodowe	9

¹ <https://kike.pl/czlonkowie/>

1. Mechanizm tzw. dostawcy wysokiego ryzyka niezgodny z Konstytucją RP

Niezgodne z Konstytucją Rzeczypospolitej Polskiej są rozwiązania ujęte w rozdziale 12a Ustawy, który wprowadza mechanizm tzw. dostawcy wysokiego ryzyka (dalej: „DWR”) i związany z nim nakaz usuwania sprzętu elektronicznego. Wypowiedzieli się na ten temat wybitni znawcy polskiego prawa konstytucyjnego i administracyjnego:

- 1) prof. dr hab. Ryszard Piotrowski², Katedra Prawa Konstytucyjnego, Wydział Prawa i Administracji Uniwersytetu Warszawskiego;
- 2) prof. zw. dr hab. Rafał Stankiewicz, Kierownik Katedry Prawa i Postępowania Administracyjnego, Wydział Prawa i Administracji Uniwersytetu Warszawskiego³;
- 3) prof. dr hab. Paweł Wajda⁴, Katedra Prawa i Postępowania Administracyjnego, Wydział Prawa i Administracji Uniwersytetu Warszawskiego;
- 4) prof. dr hab. Maciej Rogalski⁵, Rektor Uczelni Łazarskiego, radca prawny – Rogalski i Wspólnicy Kancelaria Prawna;
- 5) dr Krzysztof A. Wąsowski⁶, adwokat – Wspólnik WLP Legal, członek Warszawskiego Seminarium Aksjologii Administracji.

1.1. Opis mechanizmu tzw. dostawcy wysokiego ryzyka

Prof. Rafał Stankiewicz w następujący sposób opisał mechanizm DWR w swojej opinii:

„**3.2.1.** Stosownie do regulacji z art. 67c) Nowelizacji, skutkiem wydania decyzji w oparciu o art. 67b) Nowelizacji, tj. o uznaniu danego dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka („Decyzja”), będzie między innymi nakaz wycofania przez podmioty będące adresatami Decyzji w czasie przewidzianym w Nowelizacji (4 lub 7 lat) produktów objętych Decyzją. Zarazem, z uwagi na rygor natychmiastowej wykonalności Decyzji (*vide* art. 67b) ust. 18 Nowelizacji), proces takiego wycofywania powinien się w zasadzie rozpocząć z chwilą wydania Decyzji.

Przepisy Nowelizacji nie przewidują przy tym żadnej formy odszkodowania [...]. Powyższe odbywać się będzie na pełen koszt i ryzyko przedsiębiorców, którzy poniosą w całości ciężar zastąpienia dotychczasowego sprzętu i rozwiązań nowymi. W uzasadnieniu Nowelizacji brak jest przy tym jakichkolwiek szacunków, co do tego, na jakie koszty i ryzyka w związku z powyższym narażeni będą przedsiębiorcy.”⁷

W kolejnych punktach części 1 niniejszego pisma wskazane zostaną najważniejsze argumenty przemawiające za niezgodnością mechanizmu DWR z Konstytucją RP, które ww. Autorytety prawne wskazują w swoich opiniach.

1.2. Wyłączenie bez odszkodowania (art. 21 ust. 2 i art. 64 ust. 3 Konstytucji RP)

Uzasadniając twierdzenie o niezgodności mechanizmu DWR z art. 21 ust. 2 Konstytucji RP, prof. Rafał Stankiewicz wskazał:

„**3.2.3.** Odnosząc powyższe regulacje Nowelizacji do konstytucyjnie chronionego prawa własności (*vide* art. 21 ust. 1 Konstytucji RP) należy z całą mocą podkreślić, że skutkiem Decyzji nie będzie wprawdzie pozbawienie przedsiębiorcy prawa własności produktów, które będą dotknięte zakresem jej działania. To jednak jej skutkiem będzie ograniczenie a raczej unicestwienie użyteczności tych rzeczy z punktu widzenia celu w jakim

² https://kike.pl/wp-content/uploads/2025/06/2025_06_12-opinia-prof.-Ryszard-Piotrowski-dot.-UC32.pdf

³ <https://kike.pl/wp-content/uploads/2026/02/opinia-prawna-prof.-R.-Stankiewicza-nowelizacja-Ustawy-o-KSC-KIKE.pdf>

⁴ <https://orka.sejm.gov.pl/Druki10ka.nsf/0/5BB5CACE3B80D0D5C1258D57004E662A/%24File/1955-007.pdf>

⁵ <https://orka.sejm.gov.pl/Druki10ka.nsf/0/BA30E22CA1875E47C1258D550065F3DE/%24File/1955-006.pdf>

⁶ https://kike.pl/wp-content/uploads/2026/02/opinia_prawna_Krajowa-Izba-Komunikacji-Ethernetowej_WLP_08-02-2026.pdf

⁷ Prof. zw. dr hab. Rafał Stankiewicz, *Opinia prawna* z dnia 2 lutego 2026 r., str. 2 i 3

zostały nabyte [podkreślenie nasze]. W konsekwencji ich wartość rynkowa może spaść (co najmniej w Polsce) niemal do zera (to jest do wartości złomu), albo powyższe może wygenerować dodatkowy koszt utylizacji.

3.2.4. Prawu administracyjnemu znane są regulacje, w których uszczuplanie prawa własności, w tym poprzez obniżanie użyteczności rzeczy, łączy się z obowiązkiem wypłaty słusznego odszkodowania, co najmniej w postawi odszkodowania za szkodę rzeczywistą. Autor ma tutaj na myśli uregulowania z art. 36 ustawy z dnia 27 marca 2003 r., o planowaniu i zagospodarowaniu przestrzennym [...].

Powyższe stanowi przykład realizacji w normach prawa administracyjnego gwarancji wynikającej z art. 21 ust. 2 Konstytucji RP, zgodnie z którym wyłączenie jest dopuszczalne jedynie wówczas, gdy jest dokonywane na cele publiczne i za słusznym odszkodowaniem.

Dokładnie z takich samych względów rozwiązanie przyjęte w Nowelizacji winno łączyć się ze stosownym odszkodowaniem dla właścicieli objętych skutkami Decyzji lub co najmniej z kluczową partycypacją państwa polskiego w całkowitym koszcie wygenerowanym taką Decyzją [...]”⁸.

Z opinii prof. Rafała Stankiewicza wynika zatem, że mechanizm DWR jest niezgodny z art. 21 ust. 2 Konstytucji RP.

W podobnym tonie wypowiedział się w swojej opinii prof. Ryszard Piotrowski, który zwrócił również uwagę na niezgodność opisywanych rozwiązań z art. 64 ust. 3 Konstytucji RP:

„[...] W myśl art. 64 ust. 3 Konstytucji RP własność może być ograniczona tylko w drodze ustawy i tylko w zakresie, w jakim nie narusza ona istotny prawa własności. [...] W przypadku ograniczeń prawa własności wprowadzonych przez opiniowane przepisy ma miejsce ingerencja w treść prawa własności polegająca na tym, że zostaje zagrożone prawo własności w konsekwencji podjęcia decyzji o uznaniu dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, której skutki dotyczą przedsiębiorców telekomunikacyjnych w okolicznościach niezależnych od nich, co może doprowadzić do pozbawienia zainteresowanych zdolności wykonywania działalności gospodarczej, a więc zdolności zachowania mienia i dysponowania nim [podkreślenie nasze].”⁹

O naruszeniu art. 21 ust. 2 oraz art. 64 Konstytucji RP przez mechanizm DWR pisał w swojej opinii również prof. Paweł Wajda, wskazując m.in. że:

„Ochrona własności nie może zostać sprowadzona do fikcji [podkreślenie nasze], a państwo ma pozytywny obowiązek zapewnienia jej realnej efektywności⁶² [wstawienie nasze – treść przypisu nr 62 w Opinii: «Postanowienie TK z 6.11.2019 r., SK 21/18, OTK-A 2019, nr 68; Wyrok TK z 24.10.2001 r., SK 22/01, OTK 2001, nr 7, poz. 216.»]¹⁰

Dr Krzysztof Wąsowski zwrócił nadto uwagę, iż:

„Z perspektywy konstytucyjnej regulacja ta nosi znamiona bezprawnego wyłączenia faktycznego lub pośredniego. Mimo że Projekt nie przewiduje formalnego przeniesienia tytułu własności na rzecz Skarbu Państwa, skutek ekonomiczny i prawny dla przedsiębiorcy jest tożsamy z wyłączeniem – traci on możliwość czerpania korzyści z posiadanego składnika majątkowego [podkreślenie nasze].[...]”

Decyzja Ministra o wszczęciu procedury uznania za DWR ma charakter wysoce uznaniowy i nie jest uzależniona od wystąpienia jakiegokolwiek przesłanki technicznej, takiej jak wykrycie podatności, incydent krytyczny czy dowód na istnienie tzw. tylnych furtek (*backdoors*). Wystarczy sama ocena ryzyka oparta na kryteriach geopolitycznych. W efekcie, przedsiębiorca może zostać pozbawiony prawa do korzystania z legalnie nabytego mienia nie z powodu wadliwości sprzętu, lecz z przyczyn politycznych, leżących całkowicie poza jego kontrolą. Taka konstrukcja przepisów, pozbawiona mechanizmu odszkodowawczego, nosi znamiona wyłączenia pod pozorem regulacji administracyjnej [podkreślenie nasze]¹¹”.

⁸ *Ibidem*, str. 3 i 4.

⁹ Prof. dr hab. Ryszard Piotrowski, *Opinia o zgodności wybranych przepisów projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw z Konstytucją RP z dnia 12 czerwca 2025 r.*, str. 10 i 11.

¹⁰ Prof. dr hab. Paweł Wajda *Opinia na zasadzie amicus curiae dotycząca projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa*, Warszawa, z dnia 3 grudnia 2025 r., str. 38.

¹¹ Dr Krzysztof Wąsowski *Opinia prawna* z dnia 8 lutego 2026 r., str. 6 i 12.

Prof. Rafał Stankiewicz, prof. Ryszard Piotrowski, prof. Paweł Wajda oraz dr Krzysztof Wąsowski są zatem zgodni co do tego, że mechanizm DWR stanowi niedopuszczalną ingerencję w prawo własności, niezgodną z art. 21 ust. 2 oraz art. 63 ust. 4 Konstytucji RP.

1.3. Naruszenie zasad społecznej gospodarki rynkowej i swobody działalności gospodarczej (art. 20 i art. 22 Konstytucji RP)

Prof. Ryszard Piotrowski zwrócił także uwagę na niezgodność mechanizmu DWR z art. 20 Konstytucji:

„Projektowane rozwiązanie, wprowadzając swego rodzaju upaństwowienie podmiotów prywatnych przez arbitralne i nieproporcjonalne ograniczenie możliwości działania tych podmiotów, jest niezgodne z art. 20 Konstytucji RP, w myśl którego społeczna gospodarka rynkowa oparta na wolności działalności gospodarczej, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych stanowi podstawę ustroju gospodarczego Rzeczypospolitej Polskiej. W orzecznictwie Trybunału Konstytucyjnego znalazł wyraz pogląd, że uczynienie własności prywatnej jedną z podstaw gospodarki rynkowej wynika z zakazu powrotu do systemu, w którym dominuje własność państwowa oraz własność podmiotów powiązanych z państwem¹² [*podkreślenie nasze*] [*wstawienie nasze - treść przypisu nr 14 w Opinii: «Tak w uzasadnieniu wyroku w sprawie o sygn. K 14/99.»*]. W opiniowanym zakresie projektowane rozwiązanie wprowadza nadmierne niż dopuszczalne w społecznej gospodarce rynkowej powiązanie podmiotów prywatnych z państwem.¹²”

Podobnie wnioski w swojej opinii przedstawił prof. Paweł Wajda¹³.

Dr Krzysztof Wąsowski wskazał ponadto, że:

„Analiza art. 67b ust. 11 pkt 2 Projektu prowadzi do wniosku, że skonstruowany przez ustawodawcę mechanizm oceny dostawcy opiera się w przeważającej mierze na przesłankach o charakterze politycznym i geopolitycznym, marginalizując obiektywne kryteria techniczne. Przepis ten nakazuje Kolegium i Ministrowi badanie „prawdopodobieństwa” znajdowania się dostawcy pod wpływem państwa spoza UE lub NATO, a także ocenę ustawodawstwa tego państwa w zakresie ochrony praw człowieka czy zdolności do ingerencji w swobodę działalności gospodarczej.[...]”

Projekt pozwala na uznanie podmiotu za DWR i eliminację jego produktów z rynku nie na podstawie udowodnionych faktów – takich jak wykrycie luki w oprogramowaniu (tzw. *backdoor*), wystąpienie incydentu bezpieczeństwa czy naruszenie poufności danych – lecz na podstawie abstrakcyjnego domniemania zagrożenia wynikającego z samej lokalizacji siedziby głównej dostawcy [*podkreślenie nasze*]. [...]

Taka konstrukcja przepisów nadaje postępowaniu w sprawie DWR charakter wysoce arbitralny i uznaniowy. Organ administracji otrzymuje uprawnienie do wykluczenia legalnie działającego przedsiębiorcy z obrotu gospodarczego w oparciu o niejawne analizy służb specjalnych dotyczące polityki państwa trzeciego, a nie jakości produktów tego przedsiębiorcy. [...] Z punktu widzenia konstytucyjnego rozwiązanie to narusza zasadę swobody działalności gospodarczej (art. 20 i art. 22 Konstytucji RP) oraz zasadę równości wobec prawa. Dyskryminacja podmiotów ze względu na „paszport”, bez wykazania konkretnego zagrożenia technicznego, stanowi nieproporcjonalną ingerencję w rynek [*podkreślenie nasze*]¹⁴.

W świetle powyższych argumentów prof. Ryszarda Piotrowskiego, prof. Pawła Wajdy i dr. Krzysztofa Wąsowskiego, niezgodność mechanizmu DWR z art. 20 i 22 Konstytucji RP nie budzi wątpliwości.

1.4. Naruszenie zasady proporcjonalności (art. 2 i art. 31 ust. 3 Konstytucji RP)

Analizując mechanizm DWR w kontekście zasady proporcjonalności prof. Ryszard Piotrowski wskazał:

„Nie zgodność projektowanego rozwiązania z art. 2 Konstytucji RP polega na naruszeniu zakazu nadmiernej ingerencji wbrew zasadzie proporcjonalności stanowiących ograniczeń.[...]”

Naruszenie zasady proporcjonalności powoduje zarazem, że opiniowana regulacja jest niezgodna z dekodowaną z zasady demokratycznego państwa prawnego zasadą racjonalności działań prawodawcy. [...] Przedmiotowa regulacja jest w stanie doprowadzić do zamierzonych skutków, ale nie jest niezbędna do ochrony interesu publicznego, ponieważ możliwe jest zastosowanie takich środków, jak certyfikacja

¹² Prof. dr hab. Ryszard Piotrowski, *Op. cit.*, str. 5 i 6.

¹³ Prof. dr hab. Paweł Wajda, *Op. cit.*, str. 37.

¹⁴ Dr Krzysztof Wąsowski, *Op. cit.* Str. 13.

cyberbezpieczeństwa, czy też dywersyfikacja dostawców sprzętu i oprogramowania. Ze względu na zakres i dolegliwość ingerencji należy uznać, że efekty regulacji nie pozostają w proporcji do nakładanych ciężarów [podkreślenie nasze].¹⁵

Z kolei prof. Paweł Wajda podkreślił, że:

„Naruszona [...] 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 restrykcyjnych¹⁶”.

Prof. Rafał Stankiewicz również zwrócił uwagę na naruszenie zasady proporcjonalności w Ustawie¹⁷, przy czym powiązał ją z pozbawieniem strony możliwości realizowania prawa do obrony, o którym szerzej mowa w pkt. 1.5. niniejszego pisma.

W uzasadnieniu Ustawy próżno szukać wskazówek, dla których Ustawodawca nie sięgnął po środki mniej drastyczne, takie jak dywersyfikacja dostawców sprzętu i oprogramowania, zamiast usuwania określonych kategorii produktów i usług ICT w całości. Nie wskazano również powodu, dla którego w Polsce mechanizm DWR może dotknąć kilkunastu sektorów gospodarki zamiast elementów krytycznych sieci 5G, jak ma to miejsce w większości innych państw UE (o czym będzie mowa w pkt. 4 niniejszego pisma).

Należy również podkreślić, że okres amortyzacji urządzeń aktywnych w telekomunikacji wynosi 10 lat, podczas gdy Ustawa nakazuje wycofanie określonych kategorii sprzętu i oprogramowania w okresie 4 lub 7 lat.

1.5. Fikcyjne prawo do obrony (naruszenie art. 32 ust. 1, art. 45 ust. 1, art. 77 ust. 2 i art. 78 Konstytucji RP)

Prof. Rafał Stankiewicz w następujący sposób wyliczył powody, dla których procedura DWR pozbawia strony możliwości realizowania prawa do obrony lub drastycznie je ogranicza:

„Nowelizacja [...] zawiera także szereg uregulowań, których suma sprawia, że strony postępowania w przedmiocie Decyzji lub podmioty dotknięte jej skutkami, a taką stroną nie będące, zostają pozbawione prawa do obrony swoich praw lub co najmniej w nieakceptowalnym zakresie takie prawo zostaje im ograniczone – zarówno w postępowaniu administracyjnym, jak i sądowno-administracyjnym. Powyższe zastrzeżenia odnieść należy do:

a) sytuacji podmiotów wskazanych w art. 67b ust. 1 pkt. 1), 2) oraz 3) Nowelizacji, do których Decyzja nie jest skierowana, ale obowiązki z niej wynikające będą ich dotyczyć.

b) Jednoinstancyjności postępowania administracyjnego w przedmiocie wydania Decyzji (*vide* art. 67b ust. 19 Nowelizacji), przy jednoczesnym zawężeniu możliwości udziału w postępowaniu sądowno-administracyjnym [...], gdzie skarga rozpatrywana będzie przez sąd na posiedzeniu niejawnym (*vide* art. 67e ust. 1 Nowelizacji). Jednocześnie, możliwości skutecznego wniesienia skargi kasacyjnej będą drastycznie ograniczone albowiem skarżącemu doręczany będzie odpis wyroku z częścią uzasadnienia, która nie zawiera informacji niejawnych [...] (*vide* art. 67e ust. 2 Nowelizacji). Powyższe, w połączeniu ze specyfiką skargi kasacyjnej i zasadami formułowania w niej zarzutów, czyni ochroną sądowno administracyjną wręcz iluzoryczną. Nie wspominając już o czasie oczekiwania na rozpoznanie spraw przed WSA i NSA.

c) Wyłączenia możliwości udziału w postępowaniu w przedmiocie Decyzji właściwych organizacji społecznych, przy całkowitym wyeliminowaniu zastosowania art. 28 k.p.a. oraz 79 k.p.a. (*vide* art. 67b ust. 2 Nowelizacji).

d) Dopuszczenia – obok dostawcy – do udziału w postępowaniu w przedmiocie Decyzji wyłącznie przedsiębiorców komunikacji elektronicznej, których przychód w poprzednim roku obrotowym osiągnął co najmniej dwudziestotysięczną krotność przeciętnego wynagrodzenia ogłaszanego przez Prezesa GUS, co

¹⁵ Prof. dr hab. Ryszard Piotrowski, *Op. cit.*, str. 2 i 4.

¹⁶ Prof. dr hab. Paweł Wajda, *Op. cit.*, str. 12.

¹⁷ Prof. zw. dr hab. Rafał Stankiewicz, *Op. cit.*, str. 5.

sprawia, że pozbawieni możliwości ochrony swoich praw zostało większość spośród około 3900 przedsiębiorców telekomunikacyjnych. Mimo, że to właśnie tych mniejszych przedsiębiorców mogą dużo bardziej dotknąć skutki Decyzji. Powyższe dodatkowo stanowi rozwiązanie o charakterze dyskryminującym.

[...] Suma powyższych regulacji czyni, w ocenie Autora, postępowania administracyjne i postępowania sądowno-administracyjne w przedmiocie Decyzji postępowaniami wręcz fasadowymi, które jedynie stanowią pozór możliwości ochrony swoich praw przez podmioty dotknięte działaniem Decyzji [podkreślenie nasze]. Powyższe stanowi jednoznaczne naruszenie konstytucyjnie gwarantowanej sprawiedliwości proceduralnej w rozumieniu art. 78 Konstytucji RP, art. 45 ust. 1 Konstytucji RP, art. 77 ust. 2 Konstytucji RP, przy jednoczesnym naruszeniu zasady proporcjonalności, o jakiej mowa w art. 31 ust. 3 Konstytucji RP.¹⁸

Prof. Ryszard Piotrowski podkreślił przy tym, że:

„Zgodnie z art. 45 ust. 2 Konstytucji dopuszczalne jest wyłączenie jawności rozprawy, a nie jawności uzasadnienia. Ponadto powołany przepis przewiduje, że wyrok ogłaszany jest publicznie. Uzasadnienie jest częścią wyroku¹⁹.”

Niezgodność procedury DWR z art. 45 ust. 2 Konstytucji RP podniósł w swojej opinii również prof. Paweł Wajda²⁰. Z kolei prof. Maciej Rogalski podkreśla niezgodność opisanej procedury z art. 32 ust. 1, art. 45, art. 77 ust. 2 oraz art. 78 Konstytucji²¹.

2. Pozostałe rozwiązania niezgodne z Konstytucją RP

2.1. Polecenie zabezpieczające (art. 87 ust. 1 Konstytucji RP – źródła prawa)

Zarówno prof. Ryszard Piotrowski, jak i prof. Paweł Wajda w swoich opiniach podkreślili brak zgodności art. 67g ust. 2 dodawanego Ustawą do ustawy o krajowym systemie cyberbezpieczeństwa z art. 87 ust. 1 Konstytucji RP²². Prof. Ryszard Piotrowski wskazał przy tym, że polecenie zabezpieczające, wydawane przez właściwego ministra, dotyczy nieokreślonej liczby podmiotów kluczowych i ważnych, choć:

„[...] art. 87 ust. 1 nie zalicza poleceń ministra do źródeł prawa powszechnie obowiązującego, a więc obowiązującego te podmioty. Polecenia ministra nie są rozporządzeniami ministra. Podmioty wskazane w art. 67 g ust. 2 projektu nie są jednostkami organizacyjnie podległymi ministrowi, a zatem nie wiążą je polecenia ministra nawet, gdyby były jego zarządzeniem²³”.

Polecenie zabezpieczające posiada zatem wszystkie cechy aktu prawa powszechnie obowiązującego, choć nie zostało przewidziane w katalogu takich aktów i wydawane jest w procedurze przypominającej bardziej decyzję administracyjną niż np. rozporządzenie właściwego Ministra. Z tego powodu art. 67g ust. 2 dodawany Ustawą do ustawy o krajowym systemie cyberbezpieczeństwa jest niezgodny z art. 87 Konstytucji RP.

2.2. Metodyki nadzoru – opinia Biura Legislacyjnego Senatu RP (art. 2, 87 i 92 ust. 1 Konstytucji RP)

Eksperci Biura Legislacyjnego Senatu RP podnieśli w swojej opinii, że art. 53a ust. 2 dodawany Ustawą do ustawy o krajowym systemie cyberbezpieczeństwa, budzi wątpliwości w zakresie zgodności z art. 87 i art. 92 ust. 1 Konstytucji. Omawiany przepis wskazuje, że zakres nadzoru nad podmiotami kluczowymi, sposób jego przeprowadzania oraz kryteria oceny zostaną określone w metodykach nadzoru:

¹⁸ *Ibidem*, str. 4 i 5.

¹⁹ Prof. dr hab. Ryszard Piotrowski, *Op. cit.*, str. 14.

²⁰ Prof. dr hab. Paweł Wajda, *Op. cit.*, str. 43 i 44.

²¹ Prof. dr hab. Maciej Rogalski, Uwagi do projektu ustawy z dnia 7 października 2025 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Warszawa, 27 listopada 2025 r., str. 5-7.

²² Prof. dr hab. Ryszard Piotrowski, *Op. cit.*, str. 15; prof. dr hab. Paweł Wajda, *Op. cit.*, str. 44.

²³ Prof. dr hab. Ryszard Piotrowski, *Op. cit.*, str. 15.

„[...] elementy metodyk nadzoru w praktyce będą bezpośrednio wpływać na sytuację prawną podmiotów nadzorowanych, determinując zakres ich obowiązków, sposób weryfikacji ich realizacji oraz przesłanki negatywnej oceny w ramach nadzoru. Tym samym metodyki nadzoru nie będą miały wyłącznie charakteru wewnętrznego, organizacyjnego, lecz będą stanowić w istocie instrument konkretyzujący normy ustawowe [...] w sytuacji, gdy ustawodawca dopuszcza ustanawianie instrumentu, który w sposób wiążący wpływa na wykonywanie obowiązków ustawowych przez podmioty spoza administracji publicznej, instrument ten powinien stanowić przedmiot regulacji w przepisach powszechnie obowiązujących. Wynika to z obowiązującego w Rzeczypospolitej Polskiej systemu źródeł prawa art. 87 Konstytucji oraz z art. 92 ust. 1 Konstytucji, zgodnie z którym ustawy są wykonywane przez rozporządzenia. Pozostawienie organom administracji swobody w kształtowaniu metodyk nadzoru w formie aktów niebędących źródłami powszechnie obowiązującego prawa może prowadzić do naruszenia zasady demokratycznego państwa prawa (art. 2 Konstytucji), w szczególności zasady pewności prawa oraz zaufania obywateli do państwa i stanowionego przez nie prawa²⁴.”

Metodyki nadzoru zostały zakwalifikowane w Ustawie jako akt prawa wewnętrznego, choć ich charakterystyka odpowiada rozporządzeniu. Z tego względu Biuro Legislacyjne Senatu uznało art. 53a ust. 2 i nast., dodawane Ustawą do ustawy o krajowym systemie cyberbezpieczeństwa, za niezgodne z art. 2, 87 i 92 ust. 1 Konstytucji RP.

3. Bezprawie legislacyjne: ryzyko wielomiliardowych roszczeń odszkodowawczych wobec Skarbu Państwa

Dr Krzysztof Wąsowski stwierdził w swojej opinii, że:

„Wdrożenie wadliwych przepisów bez uprzedniej notyfikacji Komisji Europejskiej stwarza ryzyko powstania wielomiliardowych roszczeń odszkodowawczych wobec Skarbu Państwa z tytułu bezprawia legislacyjnego. [...] Zaniechanie notyfikacji technicznej skutkuje bezskutecznością przepisów technicznych wobec jednostek, co jest konsekwencją utrwalonego orzecznictwa Trybunału Sprawiedliwości UE²⁵.”

O konieczności dokonania notyfikacji technicznej ustawy pisał również w swojej opinii prof. ucz. Dr hab. Piotr Bogdanowicz (Wydział Prawa i Administracji, Uniwersytet Warszawski)²⁶.

4. Nadregulacja i arbitraż technologiczny

Ustawa wdraża unijną dyrektywę NIS²⁷ oraz wytyczne z dokumentu „5G Toolbox”²⁸. Wdrożenie 5G Toolbox jest wymogiem otrzymania kolejnej transzy środków na potrzeby Krajowego Planu Odbudowy. Tym niemniej, rozwiązania ujęte w Ustawie – szczególnie w zakresie mechanizmu DWR – znacznie wykraczają ponad wymogi prawa UE, czyli polscy przedsiębiorcy mogą znaleźć się w wyraźnie gorszej sytuacji niż przedsiębiorcy z innych państw UE np. niemieccy i czescy, z którymi konkurują. Kwestia ta była przedmiotem analizy m.in.:

- 1) prof. dr hab. Artura Nowaka-Fara²⁹, Katedra Integracji i Prawa Europejskiego, Szkoła Główna Handlowa;

²⁴ Kancelaria Senatu, Biuro Legislacyjne, *Opinia do ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk nr 609)*; Warszawa, 27 stycznia 2026 r., str. 13.
<https://www.senat.gov.pl/gfx/senat/pl/senatekspertyzy/7775/plik/609o1.pdf>

²⁵ Dr Krzysztof Wąsowski, *Op. cit.*, str. 4.

²⁶ Prof. ucz. dr hab. Piotr Bogdanowicz *Opinia prawna w sprawie obowiązku notyfikacji projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw w zakresie dotyczącym uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka*; Warszawa, 14 czerwca 2023 r. (zaktualizowana 5 lipca 2023 r. oraz 10 maja 2024 r.)

<https://orka.sejm.gov.pl/Druki10ka.nsf/0/ACD45837B9CCAE6EC1258D5500582159/%24File/1955-005.pdf>

²⁷ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148

²⁸ *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*; autor: Grupa Współpracy NIS, działająca na podstawie decyzji Komisji Europejskiej 2017/179.

²⁹ https://iptg.pl/wp-content/uploads/2026/01/Opinia-o-wykonaniu-NIS2_2-FINAL_ANF.pdf

2) firmy doradczej EY³⁰ (dawniej Ernst and Young).

W 5G Toolbox DWR dotyczy sieci 5G i krytycznych elementów w tej sieci. W Polsce DWR dotyczy wszystkich technologii sieci ruchomych sieci telekomunikacyjnych, oraz podmiotów kluczowych i ważnych z 18 różnych sektorów gospodarki. Żadne państwo członkowskie UE nie zdecydowało się na tak dalekoidące rozszerzenie tego mechanizmu.

Najbardziej niebezpieczną konsekwencją praktyczną, płynącą dla polskich przedsiębiorców z nadregulacji w zakresie DWR, może być arbitraż technologiczny, czyli sprzedawanie przez dostawców z innych państw UE droższych technologii u nich wytworzonych w warunkach, w których w tych państwach będą nabywane (tańsze) technologie pochodzące z państw trzecich uznanych w Polsce za niedopuszczalne. Jak wskazał prof. Artur Nowak-Far:

„Skutkiem takiego działania będzie – przynajmniej w zakresie samego komponentu cyfrowego i w obszarze rynku wewnętrznego Unii Europejskiej – trwałe obniżenie konkurencyjności podmiotów polskich, które będą musiały kupować technologie droższe i zwiększenie konkurencyjności podmiotów z innych państw UE, które będą mogły nabywać technologie tańsze [podkreślenie nasze]³¹”.

Najlepszą praktyką wdrażania prawa UE, rekomendowaną nawet przez Komisję Europejską, jest rezygnacja z nadregulacji³². Nakładanie, przy wdrażaniu prawa UE (w szczególności dyrektyw), obowiązków wykraczających poza wymagania określone w tym prawie powoduje, że podmioty prowadzące działalność w Polsce będą położone w gorszej sytuacji od podmiotów z innych państw członkowskich. Rezygnacja z nadregulacji zmierza do zrównania szans i warunków prowadzenia działalności gospodarczej przez polskich przedsiębiorców (zapewnienie tzw. *level playing field*) z podmiotami z innych państw członkowskich UE.

5. USA? Chiny? A może jednak Polska.

W związku z pracami nad Ustawą w prasie dyskutowane są kwestie interesów USA i Chin³³. I faktycznie, prace nad ustawą do pole walki o rynek pomiędzy zachodnimi i chińskimi Big Techami. W trakcie dyskusji medialnej nad kolejną poprawką wprowadzoną do Ustawy, a dotyczącą operatorów sieci ruchomych, eksperci rynkowi wskazywali trzy konkretne Big Techy, najbardziej zainteresowane pracami nad mechanizmem DWR³⁴.

Warto przy tym zauważyć, że Ustawę i mechanizm DWR w jego obecnym rozdmuchanym kształcie popierają przede wszystkim organizacje zrzeszające producentów sprzętu i oprogramowania z UE i NATO, które mają nadzieję odnieść największe finansowe korzyści z decyzji DWR. Do nabywania ich sprzętu mogą zostać odgórnie zmuszeni polscy MŚP, których reprezentują.

5.1. DWR to nie jest eliminacja wad w sprzęcie ICT i oprogramowaniu

Mechanizm DWR nie został skonstruowany, aby:

³⁰ <https://www.ey.com/content/dam/ey-unified-site/ey-com/pl-pl/noindex/ey-regulacje-nis2-i-5g-toolbox.pdf>

³¹ Prof. dr hab. Artur Nowak-Far, *Porównanie modeli wykonania dyrektywy NIS2 w wybranych państwach członkowskich unii europejskiej: w Austrii, Czechach, Finlandii, Niemczech, Słowacji, Słowenii, na Węgrzech i we Włoszech. Ekspertyza przygotowana dla Polskiego Towarzystwa Gospodarczego*; stan prawny: 15 sierpnia 2025 r., str. 6.

³² Por. Better Regulation Guidelines: https://commission.europa.eu/document/download/d0bbd77f-bee5-4ee5-b5c4-6110c7605476_en?filename=swd2021_305_en.pdf).

³³ Por. np. <https://www.money.pl/gospodarka/europa-w-kleszczach-miedzy-usa-i-chinami-specyficzna-rola-polski-opinia-7168650044480288a.html>

³⁴ <https://www.rp.pl/polityka/art41339511-poprawka-warta-miliardy-kto-straci-a-kto-zarobi-na-wymianie-sprzetu-w-sieciach-komorkowych>

- walczyć ze sprawcami cyberataków i podmiotami powiązanymi, ponieważ tym celom służy rozporządzenie 2019/796³⁵ i Kodeks karny;
- usuwać krytyczne wady sprzętu i oprogramowania, ponieważ do tego służy art. 32 ust. 2 obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa;
- realizować natychmiastowe działania w razie incydentu krytycznego, ponieważ w tym celu ustanowiono polecenie zabezpieczające (art. 67g dodawany do ustawy o krajowym systemie cyberbezpieczeństwa, ujęty w art. 1 pkt 76 Ustawy);

DWR w 5G Toolbox służy wyłącznie zarządzaniu ryzykiem w kontroli dostępu³⁶ oraz zakłóceń w łańcuchu dostaw³⁷ dla sieci 5G³⁸. Nakaz usuwania całych kategorii sprzętu i oprogramowania w całości jest zatem całkowicie nieadekwatnym środkiem działania. W sytuacji, gdy właściwy minister uzna danego dostawcę za obciążonego wyższym ryzykiem, powinno to uzasadniać np. odpowiednią redukcję sprzętu i oprogramowania takiego dostawcy i unikanie uzależniania się od takiego dostawcy, ale nie usuwanie sprzętu, który może być w pełni sprawny i bezpieczny. To nie politycy powinni ręcznie decydować o rozbiórce polskiej infrastruktury z powodów politycznych.

5.2. Polscy przedsiębiorcy MŚP a bezpieczeństwo narodowe

W dyskusjach nad Ustawą i interesach USA oraz Chin pomija się, że istotą bezpieczeństwa nie jest to, kto wyprodukował sprzęt, ale kto nim zarządza i go obsługuje. Strategicznie najważniejsze jest, żeby to polscy inżynierowie zarządzali urządzeniami, w których przetwarzane są dane Polaków. Tym bardziej, że i tak zdecydowana większość mikroczipów oraz innych komponentów sprzętu i oprogramowania powstaje w Azji. Nakaz usuwania sprzętu dostawców spoza UE i NATO może zatem dawać wyłącznie iluzję bezpieczeństwa, za to z pewnością w praktyce może zachwiać przedsiębiorcami MŚP:

- 1) wbrew twierdzeniom Ministerstwa Cyfryzacji i organizacji reprezentujących zachodnie Big Techy, mechanizm DWR dotknie zdecydowaną większość przedsiębiorców MŚP. W Ustawie wprowadzono zasadę, że nakaz usuwania sprzętu i oprogramowania DWR dotyczy tylko przedsiębiorców komunikacji elektronicznej o rocznych przychodach wyższych niż 10 mln zł. Tym niemniej, mechanizm ten dotyczy również wszystkich dostawców usługi DNS, bez względu na ich dochody i wielkość, a w praktyce polskiego rynku świadczenie dostępu do internetu bez własnej usługi DNS może spowodować spadek konkurencyjności firmy. Co więcej, polscy dostawcy internetu są kluczowi w mniejszych miastach, miasteczkach i wsiach, świadcząc usługi podmiotom publicznym i wielu innym podmiotom kluczowym i ważnym, które będą podlegać pod DWR. W ten sposób mechanizm DWR może zostać rozszerzony na MŚP także w drodze wymogów, które zaczną pojawiać się w przetargach publicznych lub klauzulach umownych;
- 2) Ustawa nie zawiera Oceny Skutków Regulacji w zakresie DWR, w tym w odniesieniu do wpływu na segment MŚP. W związku z tym, aby zbadać skalę zagrożenia mechanizmem DWR dla MŚP, KIKE przeprowadziła badania wśród przedsiębiorców MŚP. Z Raportu³⁹ powstałego na gruncie tych badań wynika, że ponad 80% polskich MŚP posiada w swoich zasobach ponad 50% sprzętu

³⁵ Rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

³⁶ Ryzyko „R2” w 5G Toolbox.

³⁷ Ryzyko „R5” w 5G Toolbox.

³⁸ 5G Toolbox, str. 21.

³⁹ *Raport z badania przeprowadzonego wśród przedsiębiorców telekomunikacyjnych w zakresie kosztów wymiany sprzętu i oprogramowania dostawców spoza UE i NATO w przypadku zastosowania mechanizmu dostawcy wysokiego ryzyka*; Krajowa Izba Komunikacji Ethernetowej, Warszawa, 2 lutego 2026 r.

<https://kike.pl/2026/02/raport-z-badania-nt-kosztow-wymiany-sprzetu-i-oprogramowania-dostawcow-spoza-ue-i-nato/>

dostawców spoza UE i NATO⁴⁰, który – na gruncie Ustawy – będzie usunąć łatwiej niż sprzęt pozostałych dostawców⁴¹. Łatwiejsze usunięcie sprzętu i oprogramowania dostawców spoza UE i NATO wynika z wprowadzenia do Ustawy dodatkowych przesłanek związanych z państwem pochodzenia dostawcy (tylko w przypadku dostawców spoza UE i NATO), wpływających bezpośrednio na ocenę bezpieczeństwa danego dostawcy;

- 3) z ww. Raportu KIKE wynika, że całkowite koszty związane z koniecznością wymiany sprzętu dostawców spoza UE i NATO u jednego przedsiębiorcy można oszacować na poziomie 1 128 750 PLN netto w pierwszym roku, natomiast w przeciągu 5 lat kwota ta może wynosić 2 527 750 PLN netto⁴². **Koszty dla wszystkich przedsiębiorców telekomunikacyjnych mogłyby zatem wynieść 14,4 mld zł netto w ciągu pięciu lat⁴³**. Szacunki te są znacznie zaniżone, ponieważ badanie nie dotyczyło największych przedsiębiorców telekomunikacyjnych (operatorów sieci ruchomej, międzynarodowych korporacji). Warto zestawić tę liczbę z innymi liczbami charakterystycznymi dla rynku telekomunikacyjnego:
- a. **roczne przychody** z tytułu świadczenia usługi stacjonarnego dostępu do internetu wyniosły 6,3 mld zł, z tytułu usług telefonii stacjonarnej i VoIP (w sumie) ok. 1 mld zł, a z tytułu płatnych usług telewizyjnych: 6,8 mld zł⁴⁴ – **czyli w sumie ok. 14 mld zł**.
 - b. powyższe oznacza, że praktyczne konsekwencje decyzji DWR mogą pozostawić po sobie krajobraz księżycowy wśród polskich przedsiębiorców.

W Polsce działa 2 781⁴⁵ mikro, małych i średnich dostawców szerokopasmowego internetu. Segment MŚP odpowiada za ok. 30% internetu stacjonarnego w Polsce. Pod hasłem bezpieczeństwa narodowego Ustawa wprowadza rozwiązania, które mogą mieć dla nich katastrofalne skutki, choć to dzięki MŚP możemy mówić o dużej i realnej dywersyfikacji infrastruktury telekomunikacyjnej w naszym kraju.

Podsumowując, producenci urządzeń liczą na przymusową wymianę sprzętu i oprogramowania, nawet przed upływem okresu ich amortyzacji i użyteczności, kosztem polskich przedsiębiorców. To my będziemy płacić za taką częstszą wymianę sprzętu, wymuszoną względami politycznymi.

Uzdrowienie Ustawy byłoby przy tym dość łatwe, konstruktywne propozycje poprawek zgłaszane są od dawna. Nasze propozycje były zgłaszane na każdym etapie procesu legislacyjnego, ostatni raz w czasie prac w Senacie⁴⁶.

Z przyjemnością byłbym gotowy przedstawić punkt widzenia polskich przedsiębiorców telekomunikacyjnych także osobiście, gdyby Pan Prezydent wyraził taką wolę.

Z poważaniem



Karol Skupień

Prezes Zarządu KIKE

⁴⁰ *Ibidem*, str. 20.

⁴¹ Por. pkt 1.3. niniejszego pisma oraz art. 67b ust. 11 pkt 2 wprowadzanego Ustawą do ustawy o krajowym systemie cyberbezpieczeństwa.

⁴² *Raport z badania przeprowadzonego wśród przedsiębiorców telekomunikacyjnych...*, str. 16.

⁴³ *Ibidem*, str. 20.

⁴⁴ *Raport o stanie rynku telekomunikacyjnego w 2024 r.*; Urząd Komunikacji Elektronicznej, Warszawa, czerwiec 2025 r., str. 6

https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/590/7/raport_o_stanie_rynku_2024.pdf

⁴⁵ *Ibidem*, str. 13

⁴⁶ https://www.senat.gov.pl/download/gfx/senat/pl/senatinicjatywyplik/16943/4/609_kike.pdf

Załączniki:

1. Opinia prof. dr. hab. Ryszarda Piotrowskiego (Katedra Prawa Konstytucyjnego, Wydział Prawa i Administracji Uniwersytetu Warszawskiego)
2. Opinia prof. zw. dr. hab. Rafała Stankiewicza (Kierownik Katedry Prawa i Postępowania Administracyjnego, Wydział Prawa i Administracji Uniwersytetu Warszawskiego)
3. Opinia prof. dr. hab. Pawła Wajdy (Katedra Prawa i Postępowania Administracyjnego, Wydział Prawa i Administracji Uniwersytetu Warszawskiego)
4. Opinia prof. dr. hab. Macieja Rogalskiego (Rektor Uczelni Łazarskiego)
5. Opinia dr. Krzysztofa A. Wąsowskiego (WLP Legal)
6. Kancelaria Senatu, Biuro Legislacyjne, *Opinia do ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk nr 609)*
7. Opinia prof. ucz. dr. hab. Piotr Bogdanowicz (Wydział Prawa i Administracji, Uniwersytet Warszawski)
8. Opinia prof. dr. hab. Artura Nowaka-Fara (Szkoła Główna Handlowa)
9. Wybrane fragmenty Raportu EY *Regulacje NIS2 i 5G Toolbox w Polsce. Analiza wdrożenia i porównanie z państwami UE*
10. *Raport z badania przeprowadzonego wśród przedsiębiorców telekomunikacyjnych w zakresie kosztów wymiany sprzętu i oprogramowania dostawców spoza UE i NATO w przypadku zastosowania mechanizmu dostawcy wysokiego ryzyka*; Krajowa Izba Komunikacji Ethernetowej, Warszawa, 2 lutego 2026 r.