WLP Legal
Wisdom • Law • People

OPINIA PRAWNA

Na zlecenie:
Krajowej Izby Komunikacji Ethernetowej „KIKE"

Sporządził:
Krzysztof A. Wąsowski
Doktor nauk prawnych/ Adwokat/ Wspólnik WLP Legal / członek Warszawskiego Seminarium Aksjologii Administracji / Wykładowca akademicki przedmiotów specjalistycznych z zakresu Prawa cyberbezpieczeństwa, Prawnych Aspektów Bezpieczeństwa Informacji oraz Prawa Nowych Technologii / Ekspert w dziedzinie informatyzacji administracji publicznej, procedury administracyjnej oraz publicznego prawa gospodarczego.

Warszawa, 8 lutego 2026

Wąsowski Lorenc-Pawlak
Kancelaria Prawna Sp. k.
NIP: 7011008434
REGON: 387710316
KRS: 0000873379

Aleje Jerozolimskie 99/9
02-001 Warszawa

krzysztof.wasowski@wlplegal.pl
www.wlplegal.pl

Słowniczek:

Konstytucja RP	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.).
Dyrektywa NIS2	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.
Dyrektywa TRIS	Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego.
Ustawa o KSC	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.).
Nowelizacja / Projekt	Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Druk sejmowy nr 1955), uchwalony przez Sejm RP w dniu 23 stycznia 2026 r.
5G Toolbox	Zbiór unijnych środków na rzecz cyberbezpieczeństwa sieci 5G (*EU Toolbox on 5G Cybersecurity*), opublikowany przez Grupę Współpracy NIS w styczniu 2020 r.
OSR	Ocena Skutków Regulacji dołączona do projektu Nowelizacji.
KE / Komisja	Komisja Europejska.
TSUE	Trybunał Sprawiedliwości Unii Europejskiej.
Minister	Minister właściwy do spraw informatyzacji (obecnie Minister Cyfryzacji)
Kolegium	Kolegium do Spraw Cyberbezpieczeństwa (organ opiniodawczo-doradczy Rady Ministrów)
CSIRT	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (*Computer Security Incident Response Team*), działający na poziomie krajowym (CSIRT NASK, CSIRT GOV, CSIRT MON) lub sektorowym.
DWR	Dostawca Wysokiego Ryzyka; status prawny nadawany dostawcy sprzętu lub oprogramowania w drodze decyzji administracyjnej Ministra, skutkujący obowiązkiem wycofania jego produktów z rynku.

Gold plating	Praktyka legislacyjna polegająca na implementacji prawa unijnego w sposób wykraczający poza wymagane minimum, nakładająca dodatkowe, nieobowiązkowe obciążenia na podmioty krajowe.
Vendor Lock-in	Uzależnienie od dostawcy; sytuacja, w której klient staje się zależny od produktów i usług jednego dostawcy, a zmiana dostawcy jest niemożliwa lub wiąże się z zaporowymi kosztami.
CAPEX	*Capital Expenditures*; wydatki inwestycyjne ponoszone przez przedsiębiorstwa na rozwój i odtworzenie majątku trwałego (tu: infrastruktury telekomunikacyjnej i informatycznej).

I. Wnioski

- Procedura nakazu wycofania sprzętu narusza konstytucyjną ochronę prawa własności, stanowiąc w istocie bezprawne (pośrednie) wywłaszczenie przedsiębiorców pod pozorem regulacji administracyjnej, bez zagwarantowania im słusznego odszkodowania.
- Kryteria oceny dostawcy wysokiego ryzyka (DWR) mają charakter geopolityczny i dyskryminacyjny, a ich zastosowanie w uznaniowym postępowaniu administracyjnym prowadzi do poważnych naruszeń standardów rzetelnej procedury (w tym ograniczenia realnej możliwości obrony i odniesienia się do podstaw decyzji).
- Nadanie decyzjom o uznaniu za dostawcę wysokiego ryzyka (DWR) rygoru natychmiastowej wykonalności sprawia, że sądowa kontrola tych rozstrzygnięć staje się iluzoryczna, naruszając prawo do sądu i zasady demokratycznego państwa prawnego.
- Wdrożenie wadliwych przepisów bez uprzedniej notyfikacji Komisji Europejskiej stwarza ryzyko powstania wielomiliardowych roszczeń odszkodowawczych wobec Skarbu Państwa z tytułu bezprawia legislacyjnego.
- Projekt ustawy zawiera przepisy techniczne w rozumieniu Dyrektywy 2015/1535, które nie zostały notyfikowane Komisji Europejskiej, co stanowi rażące naruszenie procedury prawodawczej UE.
- Zaniechanie notyfikacji technicznej skutkuje bezskutecznością przepisów technicznych wobec jednostek, co jest konsekwencją utrwalonego orzecznictwa Trybunału Sprawiedliwości UE.
- Projekt stanowi przykład nadmiernej regulacji (gold-plating), obejmując nieuzasadnioną liczbę około 40 tysięcy podmiotów. Na tle rozwiązań przyjmowanych w UE brak jest analogicznego rozszerzenia obowiązku usuwania sprzętu na taką skalę; przykładowo w Niemczech środki ograniczające dostawców wysokiego ryzyka wiązane są z wąsko zdefiniowaną grupą operatorów infrastruktury krytycznej (KRITIS) – 1 179 podmiotów[1].
- Ocena Skutków Regulacji (OSR) jest wadliwa, gdyż pomija koszty wymiany infrastruktury, co uniemożliwia racjonalną ocenę ekonomicznych konsekwencji ustawy.

[1] stan na 31 grudnia 2025; dane BSI: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html

- Rozszerzenie mechanizmu uznawania dostawcy za DWR na 19 sektorów gospodarki stanowi niedopuszczalne przekroczenie ram wynikających z Dyrektywy NIS2 oraz zaleceń unijnego zestawu narzędzi (5G Toolbox).
- Definicje podmiotów kluczowych i ważnych, jak również obowiązki sprawozdawcze oraz procedury kontrolne, są sformułowane nieprecyzyjnie, co generuje stan niepewności prawnej w zestawieniu z drakońskimi sankcjami finansowymi.

II. Przedmiot opinii

Przedmiotem niniejszej opinii jest dogmatycznoprawna analiza postanowień ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (uchwalona przez Sejm RP w dniu 23 stycznia 2026 r., druk sejmowy nr 1955), w kontekście implementacji Dyrektywy (UE) 2022/2555 (NIS2) oraz ryzyk dla swobody działalności gospodarczej i bezpieczeństwa prawnego przedsiębiorców.

III. Analiza prawna

(1) Projektowany obowiązek wycofania z użytkowania określonych typów produktów ICT, przewidziany w art. 67c, stanowi jedną z najdalej idących ingerencji w sferę praw majątkowych przedsiębiorców w historii polskiego prawodawstwa gospodarczego po 1989 roku. Nakaz ten, skierowany do szerokiego kręgu podmiotów (w tym przedsiębiorców telekomunikacyjnych oraz podmiotów z 19 sektorów gospodarki), skutkuje pozbawieniem właścicieli atrybutu korzystania z legalnie nabytego mienia i przymuszeniem ich do jego fizycznej likwidacji (zniszczenia).

(2) Z perspektywy konstytucyjnej, regulacja ta nosi znamiona bezprawnego wywłaszczenia 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 wywłaszczeniem – traci on możliwość czerpania korzyści z posiadanego składnika majątkowego. Zgodnie z art. 21 ust. 2 Konstytucji RP, wywłaszczenie jest dopuszczalne jedynie wówczas, gdy jest dokonywane na cele publiczne i za słusznym odszkodowaniem. Tymczasem Projekt nie przewiduje żadnego mechanizmu kompensacyjnego dla podmiotów, które zostaną zmuszone do usunięcia sprawnej i bezpiecznej technicznie infrastruktury. Brak ustawowej gwarancji odszkodowania czyni tę regulację rażąco niekonstytucyjną.

(3) Należy zwrócić uwagę na drastyczną rozbieżność między ustawowymi terminami wycofania sprzętu (4 lata dla funkcji krytycznych, 7 lat dla pozostałych) a rzeczywistym cyklem życia infrastruktury w sektorach takich jak energetyka, kolej czy telekomunikacja, gdzie okres eksploatacji urządzeń wynosi standardowo od 15 do nawet 20 lat. Nakaz usunięcia urządzeń w połowie ich cyklu życia w sytuacji, gdy zostały one nabyte zgodnie z prawem i spełniały wszelkie ówczesne normy techniczne, narusza zasadę ochrony praw nabytych oraz zasadę zaufania obywatela do państwa. Przedsiębiorcy działający w dobrej wierze nie mogą ponosić negatywnych konsekwencji zmienności polityki państwa, która retroaktywnie delegalizuje posiadane przez nich aktywa.

(4) Co więcej, ingerencja ta narusza zasadę proporcjonalności (art. 31 ust. 3 Konstytucji RP). Skoro bowiem uznanie za DWR może nastąpić w oparciu o abstrakcyjne kryteria geopolityczne (bez wykazania wadliwości sprzętu), to nakaz jego zniszczenia jest środkiem nieadekwatnym i nadmiernym. Państwo przerzuca w ten sposób cały ciężar

ryzyka geopolitycznego na podmioty prywatne, zmuszając je do ponoszenia podwójnych nakładów inwestycyjnych (CAPEX) – raz na zakup pierwotny, a drugi raz na wymuszonym zastąpieniu sprzętu nowym – co wprost godzi w istotę wolności działalności gospodarczej.

(5) Gwarancją praworządności w demokratycznym państwie jest nie tylko formalna możliwość zaskarżenia decyzji administracyjnej, ale przede wszystkim realna i efektywna ochrona sądowa. Projektowane rozwiązania, w szczególności art. 67b ust. 18, nadający decyzji Ministra o uznaniu dostawcy za dostawcę wysokiego ryzyka (DWR) rygor natychmiastowej wykonalności, czynią sądową kontrolę tych aktów iluzoryczną, naruszając istotę konstytucyjnego prawa do sądu (art. 45 ust. 1 Konstytucji RP).

(6) Tworzy to stan dokonany. Nawet jeśli po kilku latach sąd przyzna rację dostawcy i uchyli decyzję Ministra jako bezprawną (np. z powodu błędnej oceny ryzyka lub naruszenia procedury), wyrok ten nie będzie miał dla skarżącego znaczenia restytucyjnego. W międzyczasie bowiem rynek zostanie utracony, kontrakty zerwane, a infrastruktura fizycznie zdemontowana i zastąpiona rozwiązaniami konkurencji. Odszkodowanie, o które można by się teoretycznie ubiegać w odrębnym procesie cywilnym, nie przywróci przedsiębiorcy jego pozycji rynkowej ani nie naprawi szkód wizerunkowych.

(7) W polskich realiach ustrojowych średni czas oczekiwania na prawomocne rozstrzygnięcie sprawy przed sądem administracyjnym (Wojewódzki Sąd Administracyjny, a następnie Naczelny Sąd Administracyjny) wynosi od kilkunastu miesięcy do nawet kilku lat, zwłaszcza w sprawach o wysokim stopniu skomplikowania faktycznego i prawnego. Tymczasem decyzja Ministra o uznaniu za DWR nakłada na adresatów (operatorów telekomunikacyjnych, podmioty kluczowe i ważne) obowiązek natychmiastowego powstrzymania się od nabywania sprzętu oraz rozpoczęcia procesu jego wycofywania.

(8) Konstrukcja ta prowadzi do powstania stanu faktów dokonanych (*fait accompli*). W momencie, w którym sąd administracyjny przystąpi do merytorycznej oceny legalności decyzji Ministra, zaskarżona decyzja będzie już w istocie wykonana – sprzęt zostanie usunięty, umowy z dostawcą rozwiązane, a rynek przejęty przez konkurentów. Ewentualny wyrok uchylający decyzję Ministra będzie miał dla skarżącego dostawcy charakter wyłącznie platoniczny. Nie przywróci on stanu poprzedniego (*restitutio in integrum*), gdyż ponowna instalacja usuniętej infrastruktury czy odzyskanie utraconych kontraktów będzie ekonomicznie i technicznie niemożliwe.

(9) Taka sytuacja czyni sądową kontrolę administracji iluzoryczną i fasadową. Dostawca zostaje de facto pozbawiony prawa do obrony swoich interesów, gdyż mechanizm sądowy nie jest w stanie zapewnić mu ochrony przed nieodwracalnymi skutkami wadliwej decyzji administracyjnej w czasie rzeczywistym. Rozwiązanie to budzi również poważne wątpliwości w świetle art. 47 Karty Praw Podstawowych UE, który gwarantuje prawo do skutecznego środka prawnego przed sądem. Brak mechanizmu suspensywnego (wstrzymującego wykonanie decyzji) w sprawach o tak doniosłym znaczeniu gospodarczym, przy jednoczesnym oparciu decyzji na nieostrych kryteriach

politycznych, stanowi wyłom w zasadach demokratycznego państwa prawnego i narusza zasady zaufania do organów władzy publicznej. Warto dodatkowo podkreślić, że sama procedura administracyjna prowadząca do uznania dostawcy za DWR może naruszać podstawowe gwarancje k.p.a., w szczególności zasadę czynnego udziału strony w postępowaniu (art. 10 k.p.a.) oraz obowiązek wyczerpującego zebrania i rozpatrzenia materiału dowodowego (art. 77 k.p.a.), jeśli strona – z uwagi na niejawność lub ogólnikowość przesłanek – nie ma realnej możliwości zapoznania się z podstawą rozstrzygnięcia i odniesienia się do niej.

(10) Wprowadzenie do obrotu prawnego przepisów obarczonych istotnymi wadami (w tym proceduralnymi – przykładowo brakiem notyfikacji w trybie Dyrektywy 2015/1535, omówionym w dalszej części opinii) generuje systemowe ryzyko odpowiedzialności odszkodowawczej Skarbu Państwa. Przedsiębiorcy, zmuszeni do kosztownej wymiany infrastruktury na podstawie bezskutecznych przepisów, zyskają silną podstawę do dochodzenia roszczeń za tzw. bezprawie legislacyjne. W skali całej gospodarki, obejmującej sektory telekomunikacji, energetyki czy transportu, potencjalne roszczenia mogą sięgać miliardów złotych, obciążając budżet państwa kosztami błędów proceduralnych rządu.

(11) Zgodnie z art. 1 ust. 1 lit. f Dyrektywy TRIS, pojęcie „przepisu technicznego" obejmuje nie tylko specyfikacje techniczne, ale również tzw. „inne wymagania", których przestrzeganie jest obowiązkowe *de iure* lub *de facto* przy wprowadzaniu do obrotu lub używaniu produktów w państwie członkowskim. Każdy projekt aktu prawnego zawierający takie regulacje podlega bezwzględnemu obowiązkowi notyfikacji Komisji na etapie prac legislacyjnych, co wynika wprost z art. 5 ust. 1 tej dyrektywy.

(12) Analizowany Projekt – w szczególności w zakresie art. 67b oraz art. 67c – wprowadza mechanizm prawny, który w sposób bezpośredni i władczy ingeruje w obrót produktami ICT. Decyzja organu o uznaniu dostawcy za *DWR* skutkuje bowiem ustawowym zakazem wprowadzania do użytkowania nowych produktów tego dostawcy oraz bezprecedensowym nakazem fizycznego wycofania (demontażu) sprzętu już funkcjonującego w sieciach. Tego typu regulacje, wpływające na właściwości produktu lub cykl jego życia na rynku, wypełniają definicję „innych wymagań" w rozumieniu *Dyrektywy TRIS*, a zatem stanowią przepisy techniczne.

(13) Należy z całą stanowczością podkreślić, że sam fakt implementowania przez Projekt postanowień Dyrektywy NIS2 nie zwalnia państwa członkowskiego z obowiązku notyfikacji w procedurze TRIS. Projekt wprowadza bowiem dodatkowe, specyficzne wymogi krajowe (m.in. w oparciu o niewiążący *5G Toolbox*), które nie wynikają wprost z przepisów unijnych. Wprowadzenie tak restrykcyjnych zakazów dotyczących sprzętu, bez uprzedniego poddania ich procedurze notyfikacji i konsultacji z KE oraz innymi państwami członkowskimi, stanowi rażące naruszenie procedury prawodawczej UE. Oznacza to, że proces legislacyjny obarczony jest pierwotną i nieusuwalną wadą formalną.

(14) Konsekwencją naruszenia przez państwo członkowskie obowiązku notyfikacji przepisów technicznych, wynikającego z Dyrektywy TRIS, nie jest jedynie formalne uchybienie procedurom unijnym czy narażenie się na procedurę naruszeniową ze strony KE. W świetle utrwalonego i rygorystycznego orzecznictwa TSUE, zaniechanie to rodzi znacznie dalej idące skutki prawne w sferze stosowania prawa krajowego, określane mianem „sankcji bezskuteczności" (*unenforceability*).

(15) Fundamentalne znaczenie dla tej kwestii mają wyroki *TSUE* w sprawach C-194/94 (*CIA Security International*) oraz C-443/98 (*Unilever*). Trybunał przesądził w nich, że naruszenie obowiązku notyfikacji stanowi wadę proceduralną o charakterze zasadniczym, która czyni odnośne przepisy techniczne niezdatnymi do stosowania wobec jednostek. Oznacza to, że przepisy ustawy, które powinny zostać notyfikowane, a nie zostały – w tym przypadku projektowane art. 67b i art. 67c *Nowelizacji* w zakresie, w jakim wprowadzają zakazy stosowania sprzętu – nie mogą stanowić skutecznej podstawy prawnej dla jakichkolwiek decyzji administracyjnych nakładających obowiązki na podmioty prywatne.

(16) W praktyce procesowej oznacza to, że sądy krajowe mają obowiązek odmówić zastosowania nienotyfikowanego przepisu technicznego w każdym postępowaniu, w którym powołuje się na niego organ administracji. Obowiązek ten ma charakter bezwzględny i wynika z zasady pierwszeństwa prawa unijnego. Jeżeli zatem Minister wydałby decyzję o uznaniu dostawcy za DWR i nakazał usunięcie jego sprzętu na podstawie nienotyfikowanej Nowelizacji, sąd administracyjny rozpatrujący skargę na taką decyzję będzie zobligowany do uchylenia jej jako wydanej bez skutecznej podstawy prawnej.

(17) Tym samym, zaniechanie rządu w zakresie procedury notyfikacyjnej prowadzi do paraliżu legislacyjnego. Projekt w obecnym kształcie tworzy bowiem normy prawne, które – choć formalnie wejdą w życie i znajdą się w Dzienniku Ustaw – będą „martwe" (*non-existent in law*) w relacji państwo-jednostka. Operatorzy telekomunikacyjni oraz podmioty z sektorów kluczowych będą uprawnieni do skutecznego podważania każdego nakazu demontażu infrastruktury, powołując się bezpośrednio na wadę legislacyjną ustawy i orzecznictwo TSUE, co uczyni cały mechanizm usuwania sprzętu niewykonalnym w świetle prawa.

(18) Projektowana ustawa stanowi klasyczny przykład zjawiska *gold-platingu*, czyli transpozycji prawa unijnego w sposób nakładający na krajowe podmioty obciążenia wykraczające poza minimum wymagane przez dyrektywę. Choć Dyrektywa NIS2 ma na celu harmonizację poziomu cyberbezpieczeństwa w UE, polski ustawodawca zdecydował się na drastyczne rozszerzenie zakresu podmiotowego regulacji, obejmując nią szacunkowo aż 40 000 podmiotów.

(19) Analiza prawno-porównawcza wskazuje na rażącą dysproporcję między Polską a największymi gospodarkami UE. W Niemczech, posiadających PKB wielokrotnie wyższe od Polski, nowe regulacje obejmą ok. 28 000 podmiotów. We Francji szacuje się tę liczbę na 10 000 – 15 000, a w Hiszpanii na 25 000 – 33 000. Objęcie w Polsce tak szerokiej grupy

przedsiębiorców – w tym mniejszych podmiotów z sektorów takich jak przetwórstwo żywności, chemikalia czy gospodarka odpadami – nie znajduje uzasadnienia w realnej ocenie ryzyka dla bezpieczeństwa państwa. Co istotne, w państwach tych mechanizm kwalifikacji dostawcy jako dostawcy wysokiego ryzyka (DWR) w konstrukcji połączonej z powszechnym obowiązkiem fizycznego usuwania sprzętu (tzw. „rip and replace") w ogóle nie został wprowadzony. W Niemczech, gdzie w ostatnim czasie wdrożono rozwiązania pozwalające na ograniczanie lub zastępowanie sprzętu pochodzącego od dostawców wysokiego ryzyka, instrument ten jest wiązany z wąsko zdefiniowanym kręgiem operatorów infrastruktury krytycznej (KRITIS) – według danych BSI na dzień 31.12.2025 jest to 1 179 podmiotów. Na tym tle brak jest w UE przykładów rozszerzenia obowiązku usuwania sprzętu na skalę porównywalną z projektowanymi w Polsce ~40 tys. adresatów[2].

(20) Tak szerokie ujęcie definicji bezpieczeństwa narodowego prowadzi do systemowego rozmycia odpowiedzialności. Służby odpowiedzialne za cyberbezpieczeństwo (CSIRT) dysponują ograniczonymi zasobami kadrowymi i technicznymi. Zalanie ich tysiącami zgłoszeń o incydentach z podmiotów niemających strategicznego znaczenia (np. lokalne zakłady produkcyjne) doprowadzi do paraliżu decyzyjnego i odwrócenia uwagi od ochrony infrastruktury faktycznie krytycznej (energetyka, bankowość, łączność). W efekcie, zamiast wzmocnienia systemu, nastąpi jego osłabienie poprzez rozproszenie zasobów.

(21) Ponadto, nałożenie na dziesiątki tysięcy polskich przedsiębiorców restrykcyjnych obowiązków w zakresie raportowania, audytów oraz potencjalnej wymiany sprzętu (w ramach mechanizmu DWR), w połączeniu z drakońskimi karami finansowymi, wpłynie negatywnie na konkurencyjność polskiej gospodarki. W sytuacji, gdy firmy w innych państwach UE nie będą obciążone takimi wymogami, polskie podmioty znajdą się w gorszej pozycji rynkowej, co jest sprzeczne z celem harmonizacji rynku wewnętrznego.

(22) Jednym z fundamentalnych wymogów stawianych prawodawstwu w demokratycznym państwie prawnym jest zasada określoności prawa (*lex certa*), wywodzona z art. 2 Konstytucji RP. Nakazuje ona konstruowanie przepisów w sposób precyzyjny, jasny i zrozumiały dla adresatów, tak aby mogli oni przewidzieć skutki prawne swoich działań. Analiza postanowień Projektu prowadzi do wniosku, że w wielu kluczowych obszarach nie spełnia on tego standardu, tworząc stan głębokiej niepewności prawnej dla tysięcy podmiotów gospodarczych.

(23) Problemem legislacyjnym jest nieostrość kryteriów kwalifikacji do kategorii podmiotów kluczowych oraz podmiotów ważnych. Projekt przenosi ciężar identyfikacji statusu prawnego na same podmioty (samoocena), nie dostarczając jednocześnie precyzyjnych algorytmów decyzyjnych w sytuacjach granicznych. Wobec objęcia regulacją ok. 40 tysięcy podmiotów z 19 sektorów gospodarki, w tym tak zróżnicowanych jak ochrona zdrowia, produkcja żywności czy gospodarka odpadami, brak jednoznacznych

[2] *vide*: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html

wytycznych ustawowych doprowadzi do masowych sporów interpretacyjnych między przedsiębiorcami a organami nadzoru.

(24) Poważne wątpliwości budzą również procedury zgłaszania incydentów oraz mechanizmy audytowe. Przepisy Nowelizacji posługują się niedookreślonymi pojęciami w zakresie definicji „incydentu" podlegającego zgłoszeniu, co pozostawia zbyt szeroki margines uznaniowości organom CSIRT oraz organom właściwym do spraw cyberbezpieczeństwa. W praktyce oznacza to, że przedsiębiorca może zostać pociągnięty do odpowiedzialności za niezgłoszenie zdarzenia, które w jego ocenie nie spełniało przesłanek ustawowych, podczas gdy organ ex post oceni je odmiennie.

(25) Sytuację pogarsza fakt, że tak skonstruowane, nieprecyzyjne przepisy są obwarowane drakońskimi karami administracyjnymi (sięgającymi 10 mln euro lub 2% światowego obrotu) oraz osobistą odpowiedzialnością kadry zarządzającej. Nakładanie sankcji o charakterze represyjnym na podstawie niejasnych przepisów stanowi naruszenie standardów konstytucyjnych. Obywatel (przedsiębiorca) nie może ponosić negatywnych konsekwencji wadliwej techniki prawodawczej państwa.

(26) Dodatkowo, rozszerzenie definicji bezpieczeństwa narodowego na niemal całą gospodarkę powoduje, że pojęcia, które dotychczas były rezerwowane dla wąskiego katalogu infrastruktury krytycznej, stają się powszechne, co prowadzi do ich dewaluacji i rozmycia znaczeniowego. W efekcie sądy administracyjne zostaną obciążone falą odwołań od decyzji nakładających kary, w których kluczowym argumentem będzie niemożność jednoznacznego zrekonstruowania normy prawnej przez adresata, co w konsekwencji może paraliżować skuteczne egzekwowanie ustawy.

(27) Wprowadzony w Projekcie mechanizm przymusowego usuwania sprzętu i oprogramowania (tzw. mechanizm *rip and replace*), uregulowany w art. 67c, stanowi rozwiązanie o charakterze stricte krajowym, które nie znajduje bezpośredniego umocowania w przepisach Dyrektywy NIS2. Prawodawca unijny w Dyrektywie NIS2 skoncentrował się na zarządzaniu ryzykiem w łańcuchu dostaw poprzez środki techniczne i organizacyjne, nie nakładając jednak na państwa członkowskie obowiązku wprowadzania administracyjnych nakazów fizycznej eliminacji funkcjonującej infrastruktury.

(28) Polski ustawodawca uzasadnia te drakońskie środki koniecznością wdrożenia unijnego zestawu narzędzi dla sieci 5G (5G Toolbox). Należy jednak z całą mocą podkreślić, że 5G Toolbox stanowi dokument typu *soft law*, który nie jest prawnie wiążący dla państw członkowskich, a jego zakres przedmiotowy – jak sama nazwa wskazuje – ograniczony jest wyłącznie do sieci telekomunikacyjnych nowej generacji. Projekt dokonuje zatem nieuprawnionej ekstrapolacji zaleceń dotyczących wąskiego wycinka infrastruktury telekomunikacyjnej na całą gospodarkę, obejmując mechanizmem usuwania sprzętu aż 19 zróżnicowanych sektorów, w tym tak odległe od krytycznych systemów łączności jak ochrona zdrowia, zaopatrzenie w wodę czy produkcja żywności.

(29) Takie rozszerzenie zakresu przedmiotowego jest ewenementem na skalę europejską. Żadne inne państwo członkowskie UE nie zdecydowało się na nałożenie obowiązku usuwania sprzętu w 19 sektorach gospodarki w oparciu o abstrakcyjne kryteria oceny dostawcy. Prowadzi to do naruszenia zasady proporcjonalności, gdyż koszty społeczne i gospodarcze takiej operacji są niewspółmierne do potencjalnych korzyści w zakresie bezpieczeństwa. W sektorach takich jak energetyka czy transport, gdzie cykl życia urządzeń (np. sterowników przemysłowych OT) wynosi kilkanaście lat, nakaz ich wymiany przed upływem okresu eksploatacji generuje gigantyczne straty, które nie zostaną zrekompensowane przez państwo.

(30) Z perspektywy konstytucyjnej, mechanizm ten budzi zasadnicze wątpliwości w świetle ochrony prawa własności (art. 21 i art. 64 Konstytucji RP). Decyzja Ministra o wszczęciu procedury uznania za DWR ma charakter wysoce uznaniowy i nie jest uzależniona od wystąpienia jakiejkolwiek 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 wywłaszczenia pod pozorem regulacji administracyjnej.

(31) Zasadnicze wątpliwości budzi zakres przedmiotowy projektowanego mechanizmu uznawania dostawców za dostawców wysokiego ryzyka (DWR), który wykracza dalece poza ramy wyznaczone przez prawo Unii Europejskiej. Należy podkreślić, że Dyrektywa NIS2 – będąca podstawą implementacji – koncentruje się na zapewnieniu odporności systemów informacyjnych poprzez zarządzanie ryzykiem i zgłaszanie incydentów, nie obligując państw członkowskich do tworzenia procedur administracyjnych skutkujących fizyczną eliminacją konkretnych dostawców sprzętu (*vendor exclusion*) z całego rynku.

(32) Polski projektodawca, uzasadniając wprowadzenie tak drastycznych środków w art. 67b i art. 67c, powołuje się na unijny *5G Toolbox*. Jest to jednak argumentacja oparta na nadinterpretacji. Po pierwsze, *5G Toolbox* stanowi instrument prawnie niewiążący (*soft law*), a po drugie – co kluczowe – jego zakres jest ściśle ograniczony do cyberbezpieczeństwa sieci 5G. Dokument ten rekomenduje stosowanie restrykcji wobec dostawców wysokiego ryzyka wyłącznie w odniesieniu do kluczowych aktywów zdefiniowanych jako krytyczne dla sieci 5G (np. funkcja rdzenia sieci).

(33) Tymczasem Projekt dokonuje nieuprawnionej ekstrapolacji tych zaleceń na 19 sektorów gospodarki objętych Dyrektywą NIS2. Oznacza to, że rygoryzmy przewidziane dla newralgicznej infrastruktury telekomunikacyjnej zostają mechanicznie przeniesione na podmioty z branży wodociągowej, produkcji żywności, gospodarowania odpadami czy ochrony zdrowia. Takie rozwiązanie nie znajduje oparcia w żadnym akcie prawa unijnego.

(34) W efekcie dochodzi do sytuacji, w której szpital lub zakład wodociągowy może zostać zmuszony do usunięcia np. routerów czy systemów monitoringu tylko dlatego, że pochodzą one od dostawcy uznanego za DWR w kontekście sieci 5G, mimo że urządzenia te nie mają żadnego wpływu na bezpieczeństwo sieci telekomunikacyjnych państwa. Jest to działanie naruszające zasadę proporcjonalności i adekwatności środków do celu. Rozciągnięcie mechanizmu DWR na całą gospodarkę tworzy nieuzasadnione bariery rynkowe, ogranicza konkurencję i prowadzi do wzrostu kosztów funkcjonowania podmiotów kluczowych i ważnych, nie podnosząc przy tym w sposób wymierny poziomu cyberbezpieczeństwa państwa.

(35) 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.

(36) Tak sformułowane kryteria stoją w rażącej sprzeczności z zasadą neutralności technologicznej oraz zasadą dowodzenia winy w postępowaniu administracyjnym. 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.

(37) 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. W praktyce oznacza to wprowadzenie odpowiedzialności zbiorowej dla podmiotów pochodzących z określonych regionów geograficznych, niezależnie od ich rzeczywistej struktury właścicielskiej (np. spółki prywatne, akcjonariat pracowniczy) czy stosowanych standardów bezpieczeństwa (np. certyfikaty NESAS, *Common Criteria*).

(38) 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. Ponadto, w świetle prawa unijnego, wprowadzanie takich barier o charakterze politycznym może zostać uznane za naruszenie zasad konkurencji na jednolitym rynku cyfrowym, gdyż faworyzuje dostawców z określonych bloków politycznych kosztem innych, nie oferując przy tym wymiernego wzrostu poziomu bezpieczeństwa sieci i systemów informatycznych.

(39) Jednym z fundamentalnych standardów konstytucyjnych, wywodzonym z zasady demokratycznego państwa prawnego (art. 2 Konstytucji RP), jest zasada określoności prawa (*lex certa*). Nakłada ona na ustawodawcę obowiązek konstruowania przepisów w sposób precyzyjny, jasny i zrozumiały dla adresatów, tak aby mogli oni bez trudności zrekonstruować normę prawną i przewidzieć konsekwencje swoich działań. Analiza postanowień Projektu prowadzi do wniosku, że w wielu kluczowych obszarach nie spełnia on tego wymogu, tworząc stan głębokiej niepewności prawnej dla tysięcy podmiotów gospodarczych.

(40) Podstawowym źródłem ryzyka interpretacyjnego jest nieostrość kryteriów kwalifikacji podmiotów do kategorii podmiotów kluczowych oraz podmiotów ważnych. Projekt przerzuca ciężar identyfikacji statusu prawnego na samych przedsiębiorców (mechanizm samooceny), nie dostarczając jednocześnie precyzyjnych i rozłącznych definicji, zwłaszcza w odniesieniu do podmiotów działających w stykach różnych sektorów lub grup kapitałowych. Wobec objęcia regulacją szacunkowo 40 tysięcy podmiotów z 19 zróżnicowanych sektorów – od energetyki po produkcję żywności – brak jednoznacznych wytycznych ustawowych doprowadzi do chaosu kompetencyjnego i masowych sporów między biznesem a organami nadzoru co do zakresu obowiązków ustawowych.

(41) Kolejnym obszarem niepewności są procedury zgłaszania incydentów. Przepisy Nowelizacji posługują się niedookreślonymi pojęciami przy definiowaniu incydentu podlegającego obowiązkowemu raportowaniu. Pozostawia to zbyt szeroki margines uznaniowości zarówno dla podmiotów zobowiązanych, jak i dla organów CSIRT. Przedsiębiorca staje przed dylematem: raportować każde drobne zdarzenie (paraliżując pracę CSIRT) czy ryzykować karę za niezgłoszenie incydentu, który organ ex post uzna za istotny. Brak sztywnych parametrów (np. kwantyfikowalnych progów skutków incydentu) narusza pewność obrotu gospodarczego.

(42) Wątpliwości budzą również mechanizmy audytów i kontroli. Projekt nie precyzuje standardów technicznych, według których mają być przeprowadzane audyty bezpieczeństwa, ani kwalifikacji audytorów w sposób wystarczający. Stwarza to ryzyko dowolności w ocenie spełniania wymogów ustawy przez poszczególnych kontrolerów. W sytuacji, gdy wynik audytu może decydować o nałożeniu wielomilionowych kar, brak jasnych procedur odwoławczych i standardów kontrolnych jest niedopuszczalny.

(43) Zagrożenie to jest tym bardziej istotne, że naruszenie niejasnych przepisów Projektu obwarowane jest drakońskimi karami pieniężnymi (sięgającymi 10 mln euro lub 2% światowego obrotu rocznego) oraz osobistą odpowiedzialnością kierowników podmiotów. Nakładanie sankcji o charakterze represyjnym w oparciu o przepisy nieostre i budzące wątpliwości interpretacyjne stanowi rażące naruszenie standardów ochrony prawnej jednostki. Przedsiębiorca nie może ponosić negatywnych konsekwencji wadliwej i nieprecyzyjnej techniki legislacyjnej państwa.

(44) Przedłożony Projekt ustawy (uchwalony już przez Sejm RP i Senat RP), choć deklaratywnie mający na celu transpozycję unijnej Dyrektywy NIS2, w rzeczywistości

stanowi próbę wprowadzenia do polskiego porządku prawnego mechanizmów o charakterze politycznym, wykraczających dalece poza ramy harmonizacji wymaganej przez prawo Unii Europejskiej. Fundamentalnym błędem legislacyjnym, rzutującym na całą konstrukcję ustawy, jest zaniechanie notyfikacji przepisów technicznych Komisji Europejskiej. Jak wykazano w toku analizy, regulacje dotyczące nakazu wycofania sprzętu stanowią „inne wymagania" w rozumieniu Dyrektywy TRIS, a ich pominięcie w procedurze notyfikacyjnej skutkuje sankcją bezskuteczności. Oznacza to, że kluczowe instrumenty ustawy mogą stać się "martwym prawem", niemożliwym do wyegzekwowania przed sądami krajowymi, co podważa sens całego procesu legislacyjnego.

(45) Niezależnie od wad formalnych, Projekt stanowi jaskrawy przykład nadmiernej regulacji (*gold-plating*). Objęcie reżimem ustawy blisko 40 tysięcy podmiotów stawia Polskę w pozycji europejskiego lidera biurokracji w obszarze cyberbezpieczeństwa, wyprzedzając gospodarki znacznie większe, takie jak niemiecka czy francuska. Tak szerokie zakreślenie kręgu adresatów, w połączeniu z ograniczonymi zasobami kadrowymi krajowych zespołów CSIRT, grozi paraliżem systemu reagowania na incydenty. Służby odpowiedzialne za bezpieczeństwo cyfrowe państwa, zamiast koncentrować się na ochronie infrastruktury krytycznej, zostaną obciążone nadzorem nad tysiącami podmiotów o marginalnym znaczeniu dla bezpieczeństwa narodowego.

(46) Szczególny niepokój budzi mechaniczna implementacja zaleceń dokumentu *5G Toolbox* – aktu niewiążącego i sektorowego – na 19 zróżnicowanych gałęzi gospodarki. Rozciągnięcie rygorystycznych wymogów, projektowanych pierwotnie dla rdzenia sieci 5G, na sektory takie jak ochrona zdrowia, zaopatrzenie w wodę czy produkcja żywności, narusza zasadę proporcjonalności. Nie istnieje racjonalne uzasadnienie dla nakładania na szpitale czy zakłady komunalne obowiązku usuwania sprzętu w oparciu o kryteria geopolityczne, zwłaszcza gdy sprzęt ten nie pełni funkcji krytycznych w rozumieniu telekomunikacyjnym.

(47) Sam mechanizm uznawania dostawcy za DWR oparty został na przesłankach dyskryminujących, odchodząc od paradygmatu oceny technicznej na rzecz oceny politycznej. Uzależnienie statusu dostawcy od „prawdopodobieństwa" znajdowania się pod wpływem państwa trzeciego, bez konieczności udowodnienia faktycznych podatności sprzętu czy wrogich działań, stanowi zaprzeczenie zasady neutralności technologicznej. Taka konstrukcja przepisów tworzy niebezpieczny precedens, w którym o bycie albo niebycie na rynku decyduje paszport korporacyjny, a nie jakość i bezpieczeństwo oferowanych technologii.

(48) Konsekwencją uznania za DWR jest drastyczna ingerencja w prawo własności, przybierająca formę faktycznego wywłaszczenia bez odszkodowania. Nakaz usunięcia legalnie nabytego, sprawnego i posiadającego wymagane certyfikaty sprzętu przed upływem jego technicznego cyklu życia, godzi w zasadę zaufania obywatela do państwa oraz ochronę praw nabytych. Dla sektorów charakteryzujących się długim horyzontem inwestycyjnym, takich jak energetyka czy kolej, konieczność przedwczesnej wymiany

infrastruktury oznacza gigantyczne straty finansowe, których *Projekt* w żaden sposób nie rekompensuje.

(49) Sytuację pogarsza iluzoryczny charakter sądowej kontroli decyzji administracyjnych wydawanych w tym trybie. Nadanie decyzjom Ministra rygoru natychmiastowej wykonalności sprawia, że wniesienie skargi do sądu nie wstrzymuje procesu usuwania sprzętu. Biorąc pod uwagę przewlekłość postępowań sądowych w Polsce, przedsiębiorca może wygrać sprawę po kilku latach, lecz wyrok ten będzie miał znaczenie wyłącznie historyczne, gdyż jego pozycja rynkowa zostanie już nieodwracalnie zniszczona. Stanowi to naruszenie istoty konstytucyjnego prawa do sądu, które wymaga, aby ochrona prawna była efektywna, a nie tylko teoretyczna.

(50) Nie bez znaczenia pozostaje również jakość legislacyjna Projektu w zakresie definicji i obowiązków sprawozdawczych. Niejasne kryteria rozróżnienia podmiotów kluczowych i ważnych oraz niedookreślone procedury zgłaszania incydentów, w zestawieniu z drakońskimi karami pieniężnymi, tworzą stan głębokiej niepewności prawnej. Przedsiębiorcy, działając pod presją sankcji sięgających milionów euro oraz osobistej odpowiedzialności karnej, zmuszeni będą do podejmowania działań asekuracyjnych, co w dłuższej perspektywie hamować będzie procesy cyfryzacji i innowacyjności polskiej gospodarki.

(51) Krytycznej oceny wymaga także warstwa analityczna towarzysząca ustawie. Dołączona Ocena Skutków Regulacji (OSR) ma charakter fasadowy, pomijając kluczowe kategorie kosztów ponoszonych przez sektor prywatny i samorządowy. Wprowadzanie reformy o tak doniosłym znaczeniu gospodarczym bez rzetelnego bilansu zysków i strat, z ukryciem rzeczywistych kosztów społecznych (np. w cenach usług czy kosztach funkcjonowania szpitali), świadczy o instrumentalnym traktowaniu procesu legislacyjnego.

(52) Finalnie, należy stwierdzić, że zaproponowane w toku prac parlamentarnych środki łagodzące, takie jak dwuletnie odroczenie kar, mają charakter pozorny. Nie rozwiązują one istoty problemu, jakim jest konieczność fizycznej wymiany infrastruktury w nierealistycznych terminach. Bez wprowadzenia klauzuli *grandfathering* (ochrony sprzętu zastanego) oraz przywrócenia technicznego charakteru oceny dostawców, ustawa pozostanie aktem szkodliwym gospodarczo i wątpliwym konstytucyjnie, narażając Polskę na konflikt prawny z instytucjami unijnymi oraz falę pozwów odszkodowawczych.