

Warszawa, dnia 27 lutego 2026 r.

DKKIKE-2254

Szanowny Pan
Łukasz Wojewoda
Dyrektor Departamentu Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

Dot.: konsultacji publicznych unijnego aktu o cyberbezpieczeństwie

Szanowny Panie Dyrektorze,

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”), uprzejmie dziękuję za ogłoszenie publicznych konsultacji dotyczących unijnego aktu o cyberbezpieczeństwie (dalej: „CSA2” lub „projekt”). Praktyka, polegająca na konsultowaniu się z uczestnikami rynku przed przedstawieniem stanowiska polskiego Rządu na forum Unii Europejskiej zasługuje na pełne poparcie izb gospodarczych.

W naszym stanowisku nie wypowiemy się na temat organizacji oraz mandatu ENISA, lecz skupimy się na tytule IV CSA2, dotyczącym bezpieczeństwa łańcuchów dostaw oraz mechanizmu i konsekwencji uznania państw trzecich jako budzących obawy w zakresie cyberbezpieczeństwa.

Choć cel zapewnienia bezpieczeństwa unijnych łańcuchów dostaw ICT jest bezsprzecznie uzasadniony, **mechanizm zaproponowany w tytule IV CSA2 nie tylko jest (częściowo) niezgodny z prawem pierwotnym UE, prawami człowieka i Konstytucją RP, ale również nie służy realizacji celu zabezpieczenia łańcucha dostaw.** Zabezpieczenie łańcucha dostaw nie polega na tym, że nakazuje się usuwanie komponentów z tego łańcucha łańcuchu. Takie podejście generuje potężne zakłócenia, dając **jedynie iluzję bezpieczeństwa, a w praktyce samo w sobie stanowi największe zagrożenie dla ciągłości oraz stabilności łańcucha dostaw.** Co więcej, art. 103 ust. 1 i 9 oraz art. 110 CSA2 stanowią środki w istocie sankcyjne, przy czym karane są nie podmioty, które zawiniły, lecz ich kontrahenci. Stanowi to pogwałcenie zasady *nulla poena sine culpa* (wywodzonej z art. 7 Europejskiej Konwencji o Ochronie Praw Człowieka (dalej: „EKPC”).

¹ <https://kike.pl/czlonkowie/>

Spis treści

1. Największa zaleta CSA2: decyzja na poziomie UE jako antidotum na tendencje w zakresie ew. POLEXITu (poparcie).....	3
2. Największa wada CSA2: art. 103 ust. 1 i 7 oraz art. 110 CSA2 niezgodne z EKPC, Traktatami UE i Konstytucją RP (sprzeciw)	3
2.1. Opis art. 110 ust. 1 i 7 oraz art. 110 CSA2.....	3
2.2. Europejska Konwencja o Ochronie Praw Człowieka (art. 6 i 7, art. 1 Protokołu nr 1)	4
2.3. Naruszenie Traktatów unijnych i Karty praw podstawowych UE	4
2.3.1. Naruszenie zasad kompetencji powierzonych i proporcjonalności (art. 5 TUE).....	4
2.3.2. Naruszenie zasady ochrony uzasadnionych oczekiwań	4
2.3.3. Naruszenie prawa własności (art. 17 KPP) poprzez <i>de facto</i> wywłaszczenie bez odszkodowania	5
2.3.4. Naruszenie prawa do skutecznego środka prawnego i rzetelnego procesu sądowego (art. 47 KPP)	5
2.3.5. Naruszenie swobody przedsiębiorczości (art. 49 TUE), wolności prowadzenia działalności gospodarczej (art. 16 KPP) i zasady proporcjonalności (art. 52 ust. 1 KPP).....	5
2.4. Niezgodność z Konstytucją Rzeczypospolitej Polskiej	6
2.4.1. Naruszenie prawa własności i zasady wywłaszczenia za słusznym odszkodowaniem (art. 21 ust. 2, art. 64 i art. 31 ust. 3 Konstytucji RP)	6
2.4.2. Naruszenie swobody działalności gospodarczej i zasady proporcjonalności (art. 20, art. 22 i art. 31 ust. 3 Konstytucji RP).....	6
2.4.3. Naruszenie prawa do sądu (art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP).....	6
2.5. Podsumowanie rozważań.....	7
3. Art. 99 ust. 3 jako zaprzeczenie idei pełnej harmonizacji (sprzeciw).....	7
4. Art. 100 i nast. projektowanego aktu – obejście przepisów TFUE przez Komisję (sprzeciw).....	8
4.1. Art. 114 TFUE jako niewłaściwa podstawa prawna.....	9
4.2. Art. 215 TFUE jako właściwa podstawa prawna (<i>lex specialis</i>).....	9
5. Aprobata dla katalogu zniuansowanych środków zaradczych z art. 103 ust. 2 (poparcie)	10
6. Naruszenie swobody działalności gospodarczej i fundamentalnych zasad proceduralnych (art. 105 CSA2) (sprzeciw).....	10

1. Największa zaleta CSA2: decyzja na poziomie UE jako antidotum na tendencje w zakresie ew. POLEXITU (poparcie)

W pierwszej kolejności wypada podkreślić, że jako Izba popieramy ideę, aby wyznaczanie dostawców wysokiego ryzyka (DWR) miało miejsce na poziomie unijnym. Rozdrobnienie takich ustaleń pomiędzy państwami członkowskimi nieuchronnie prowadziło do:

- **zróźnicowania warunków konkurencji** pomiędzy państwami członkowskimi, czyli zaprzeczenia zasady równych szans dla przedsiębiorców (tzw. *level-playing field*),
- postawienia **przedsiębiorców krajowych** (prowadzących działalność tylko w jednym państwie członkowskim) w wyraźnie gorszej sytuacji w porównaniu z międzynarodowymi korporacjami, które płynnie mogłyby korzystać z tzw. **arbitrażu technologicznego** i bez większych strat przenosić sprzęt zakazany w jednym państwie do innego państwa, gdzie takiego zakazu nie ma.

Oba ww. zjawiska są strategicznie groźne wręcz dla członkostwa Polski w Unii Europejskiej. W sytuacji, gdy Europa buduje jeden wspólny rynek bez granic wewnętrznych, wyraźnie trudniejsze prowadzenie działalności w jednych państwach niż w innych oraz **pośrednie faworyzowanie międzynarodowych korporacji kosztem przedsiębiorców krajowych, mogłoby zniechęcać do integracji europejskiej.**

Regulacje w zakresie DWR mogą wiązać się potencjalnie z dużymi kosztami dla przedsiębiorców. Stoimy na stanowisku, że taka decyzja powinna zapadać na poziomie UE, ponieważ gdyby decyzja DWR zapadła na poziomie kraju, szczególnie jeżeli miałaby szeroki zakres, posiadałaby ona potencjał kropli przepełniającej czarę goryczy i rozbudzającej trend spadkowy dla poparcia członkostwa Polski w UE.

2. Największa wada CSA2: art. 103 ust. 1 i 7 oraz art. 110 CSA2 niezgodne z EKPC, Traktatami UE i Konstytucją RP (sprzeciw)

2.1. Opis art. 110 ust. 1 i 7 oraz art. 110 CSA2

KIKE stoi na stanowisku, że projektowane przepisy, a w szczególności art. 103 ust. 1 i 7 oraz art. 110, wprowadzają mechanizmy o bezprecedensowej skali ingerencji w prawa majątkowe przedsiębiorców:

- **Kompetencje Komisji Europejskiej wynikające z art. 103 ust. 1 i 7 projektu:** Przepisy te przyznają Komisji Europejskiej kompetencję do ustanowienia, w drodze aktu wykonawczego, całkowitego zakazu używania, instalowania lub integrowania komponentów ICT pochodzących od dostawców uznanych za dostawców wysokiego ryzyka.
- **Bezpośrednie zakazy wynikające z art. 110 projektu:** W odniesieniu do kluczowych sektorów gospodarki, zakazy te będą obowiązywały wprost z mocy samego rozporządzenia, co stanowi jeszcze dalej idącą i bardziej automatyczną ingerencję.

W obu przypadkach na użytkowników nałożony zostanie **obowiązek usunięcia wskazanych komponentów w określonych okresach przejściowych.**

Projektowane regulacje nie przewidują **żadnej formy odszkodowania ani rekompensaty** dla podmiotów dotkniętych tym *de facto* wywłaszczeniem. Mówimy o wywłaszczeniu, ponieważ w tym przypadku dochodzi do **unicestwienia użyteczności rzeczy z punktu widzenia celu, w jakim została nabyta, a jej wartość rynkowa spada niemal do zera.**

W ten sposób projekt przerzuca wszelkie koszty wynikające z dokonanego wywłaszczenia bezpośrednio na użytkowników (podmioty kluczowe i ważne). Stanowi to w istocie nałożenie na te podmioty *de facto* potencjalnie **wysokiej sankcji majątkowej za korzystanie ze sprzętu, który w momencie nabycia był w pełni legalny.**

2.2. Europejska Konwencja o Ochronie Praw Człowieka (art. 6 i 7, art. 1 Protokołu nr 1)

Z punktu widzenia standardów strasburskich, taka konstrukcja prawna uderza w podstawowe gwarancje ochrony jednostki przed arbitralnością państwa:

- **Ochrona własności (Art. 1 Protokołu nr 1):** Przedsiębiorca, nabywając legalnie komponenty, uzyskuje „mienie”. Zmuszanie go do ich usunięcia na własny koszt lub nakładanie kar za ich posiadanie bez rekompensaty jest formą nieproporcjonalnej ingerencji w prawo własności.

[**Wyrok: Sporrong i Lönnroth przeciwko Szwecji (skarga 7151/75)** – ETPCz uznał, że ingerencja w prawo własności musi zachowywać „sprawiedliwą równowagę” i nie może nakładać na jednostkę nadmiernego, indywidualnego ciężaru.]

- **Prawo do rzetelnego procesu (Art. 6):** Jeśli sankcje administracyjne są de facto represyjne (bardzo wysokie kary finansowe), podlegają one standardom procesu karnego. Karanie kogoś za czyny/wady, na które nie miał wpływu i których nie mógł przewidzieć w momencie zakupu, narusza fundament sprawiedliwości.

[**Wyrok: Jussila przeciwko Finlandii (skarga nr 73053/01)** – ETPCz orzekł, że dotkliwe kary administracyjne o charakterze represyjnym muszą podlegać gwarancjom rzetelnego procesu z art. 6 EKPC, co wyklucza automatyzm sankcji i wymaga od sądu pełnego zbadania proporcjonalności kary oraz stopnia winy ukaranego podmiotu.]

- **Zasada pewności prawa i przewidywalności kar (Art. 7):** Choć dotyczy głównie prawa karnego, ETPCz stosuje ją do dotkliwych kar administracyjnych. Prawo musi być przewidywalne – przedsiębiorca nie może być karany za działanie, które w momencie podejmowania było w pełni legalne i zgodne z normami technicznymi.

[**Wyrok: G.I.E.M. S.R.L. i inni przeciwko Włochom (skarga 1828/06)** – Trybunał wskazał, że sankcje o charakterze karnym (a za takie uznaje się dotkliwe administracyjne kary pieniężne) wymagają istnienia związku intelektualnego (winy lub przynajmniej przewidywalności) między sprawcą a czynem.]

2.3. Naruszenie Traktatów unijnych i Karty praw podstawowych UE

2.3.1. Naruszenie zasad kompetencji powierzonych i proporcjonalności (art. 5 TUE)

Artykuł 5 TUE ustanawia fundamentalne zasady, zgodnie z którymi Unia działa wyłącznie w granicach kompetencji przyznanych jej przez państwa członkowskie w Traktatach (zasada przyznania) oraz że zakres i forma jej działań nie wykraczają poza to, co jest konieczne do osiągnięcia celów Traktatów (zasada proporcjonalności).

Przyjęcie tak drastycznych środków, jak nakaz usunięcia legalnie nabytego mienia, bez wykazania, że mniej inwazyjne środki są niewystarczające, stanowi działanie nieproporcjonalne. Rodzi to poważne wątpliwości, czy instytucje UE nie działają *ultra vires*, czyli poza granicami przyznanych im kompetencji. Co więcej, zgodnie z art. 5 ust. 4 TUE, nakładając obowiązki, należy wybierać środki najmniej uciążliwe. Karanie użytkownika komponentu ICT zamiast nadzoru nad importerem/dostawcą narusza tę zasadę (por. **wyrok w sprawie C-210/16 (Wirtschaftsakademie Schleswig-Holstein)** – TSUE podkreślił, że odpowiedzialność podmiotów musi być proporcjonalna do ich faktycznego wpływu na naruszenie i możliwości technicznych kontroli nad sytuacją).

2.3.2. Naruszenie zasady ochrony uzasadnionych oczekiwań

Naruszenie tej zasady wynika z de facto sankcyjnego charakteru nakazu usuwania komponentów ICT bez odszkodowania przez podmioty, które nie ponoszą winy za wadliwość komponentu objętego nakazem usunięcia oraz które nabyły ten komponent w dobrej wierze, gdy jego legalność nie budziła wątpliwości. Zgodnie z ugruntowaną linią orzecniczą TSUE (por. **wyrok w sprawie C-17/03 VEMW**), zasada pewności prawa stoi na przeszkodzie wprowadzaniu regulacji, które w sposób nieprzewidywalny nakładają na przedsiębiorców

drastyczne ciężary finansowe, **niweczając ich uzasadnione oczekiwania co do legalności wcześniej podjętych inwestycji.**

2.3.3. Naruszenie prawa własności (art. 17 KPP) poprzez *de facto* wywłaszczenie bez odszkodowania

Projektowane przepisy art. 103 ust. 1 i 7 CSA2, przewidują, że Komisja Europejska będzie mogła w drodze aktów wykonawczych zakazać podmiotom z określonych sektorów gospodarki korzystania z komponentów ICT pochodzących od tzw. dostawców wysokiego ryzyka. Co więcej, akty te mają nakładać na użytkowników obowiązek usunięcia już posiadanych i użytkowanych komponentów w określonych okresach przejściowych. Podobny skutek jest przewidziany w art. 110 CSA2.

Taka regulacja stanowi w istocie formę ***de facto* wywłaszczenia** podmiotów unijnych, w tym polskich, które legalnie nabyły i wykorzystują w swojej działalności wskazane komponenty. Pojęcie wywłaszczenia należy bowiem rozumieć szeroko, obejmując nie tylko formalne przejęcie własności przez państwo, ale również takie środki, których skutki są równoważne z pozbawieniem prawa do korzystania z własności. Właściciele, mimo zachowania tytułu prawnego, zostają faktycznie pozbawieni możliwości korzystania ze swojego mienia, którego wartość ekonomiczna zostaje zredukowana do zera.

Powyższe stoi w jawnej sprzeczności z **art. 17 ust. 1 KPP**, który stanowi:

„Każdy ma prawo do władania, używania, rozporządzania i przekazania w drodze spadku swojego mienia nabytego zgodnie z prawem. Nikt nie może być pozbawiony swojego mienia, chyba że w interesie publicznym i w przypadkach oraz na warunkach przewidzianych w ustawie, za słusznym odszkodowaniem w odpowiednim czasie za jego utratę. Korzystanie z mienia może być regulowane przez ustawę w zakresie, w jakim jest to konieczne dla interesu ogólnego.”

Kluczowe punkty naruszenia art. 17 KPP:

- **Brak słusznego odszkodowania:** Projekt CSA2 nie przewiduje żadnej formy rekompensaty ani odszkodowania dla podmiotów dotkniętych obowiązkiem usunięcia sprzętu. Całość kosztów związanych z wywłaszczeniem (zakup nowego sprzętu, demontaż starego, straty operacyjne) jest przerzucana na przedsiębiorców. Jest to bezpośrednie naruszenie wymogu „słusznego odszkodowania” zawartego w art. 17 KPP.
- **Ingerencja w istotę prawa własności:** Nakaz usunięcia sprzętu jest środkiem, który pozbawia właściciela kluczowych atrybutów prawa własności – prawa do używania i czerpania pożytków z mienia.

2.3.4. Naruszenie prawa do skutecznego środka prawnego i rzetelnego procesu sądowego (art. 47 KPP)

Projektowana procedura w ramach CSA2 budzi również poważne wątpliwości z perspektywy prawa do sądu, gwarantowanego przez art. 47 KPP.

Brak drogi sądowej dla wywłaszczonych podmiotów: Projekt nie przewiduje skutecznej drogi sądowej dla podmiotów (użytkowników sprzętu), które zostaną bezpośrednio dotknięte skutkami aktu Komisji. Nie mają formalnej możliwości kwestionowania aktów, które prowadzą do ich faktycznego wywłaszczenia. Samo prawo do bycia wysłuchanym (przewidziane w art. 106 projektu) nie jest w żadnym wypadku równoznaczne z gwarancją rozpatrzenia sprawy przez niezależny sąd.

2.3.5. Naruszenie swobody przedsiębiorczości (art. 49 TUE), wolności prowadzenia działalności gospodarczej (art. 16 KPP) i zasady proporcjonalności (art. 52 ust. 1 KPP)

Swoboda przedsiębiorczości, ujęta w art. 49 TFUE, stoi na przeszkodzie sankcjom uderzającym w konkretne łańcuchy dostaw bez technicznego uzasadnienia, ponieważ naruszają one równe warunki konkurencji (por. **wyrok w sprawie C-390/18 (Airbnb Ireland)** – dotyczy wprowadzie innej branży, ale TSUE konsekwentnie wskazuje, że nieproporcjonalne restrykcje wobec usługodawców społeczeństwa informacyjnego naruszają swobody traktatowe).

Regulacje zawarte w projekcie CSA2 stanowią nieproporcjonalną ingerencję w wolność prowadzenia działalności gospodarczej, chronioną przez art. 16 KPP.

Kluczowe punkty naruszenia art. 16 i 52 KPP:

- **Nieproporcjonalność środka:** Nakaz całkowitego usunięcia sprzętu jest środkiem najdalej idącym i ostatecznym. Nie przewidziano rozwiązań mniej restrykcyjnych, które mogłyby osiągnąć cel w postaci zapewnienia cyberbezpieczeństwa (np. certyfikacja, audyty, ograniczenie stosowania sprzętu tylko w krytycznych elementach sieci).
- **Naruszenie istoty wolności gospodarczej:** Dla wielu przedsiębiorców przymusowa, kosztowna wymiana kluczowej infrastruktury ICT może oznaczać realne zagrożenie dla kontynuacji działalności, a tym samym naruszenie samej istoty wolności jej prowadzenia.

2.4. Niezgodność z Konstytucją Rzeczypospolitej Polskiej

2.4.1. Naruszenie prawa własności i zasady wywłaszczenia za słusznym odszkodowaniem (art. 21 ust. 2, art. 64 i art. 31 ust. 3 Konstytucji RP)

Nakaz usunięcia z infrastruktury przedsiębiorcy w pełni sprawnych i legalnie nabytych komponentów ICT, wyłącznie z powodu zakwalifikowania ich producenta jako „dostawcy wysokiego ryzyka”, stanowi formę **wywłaszczenia *de facto***. Pojęcie wywłaszczenia należy rozumieć szeroko (funkcjonalnie), jako każde działanie władzy publicznej prowadzące do odebrania lub istotnego ograniczenia prawa do korzystania z własności. W tym przypadku dochodzi do **unicestwienia użyteczności rzeczy z punktu widzenia celu, w jakim została nabyta, a jej wartość rynkowa spada niemal do zera**.

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 CSA2 nie przewiduje jakiegokolwiek formy rekompensaty dla przedsiębiorców zmuszonych do poniesienia ogromnych kosztów związanych z wymianą infrastruktury, często przed upływem jej okresu amortyzacji. Całość ciężaru finansowego tej operacji zostaje przerzucona na podmioty, które nie miały żadnego wpływu na przyczyny podjęcia decyzji przez Komisję. Taka regulacja, pozbawiająca przedsiębiorców prawa do odszkodowania, jest wprost sprzeczna z gwarancjami ochrony własności, która nie może być sprowadzona do fikcji (por. **wyrok TK z 24.10.2001 r., SK 22/01**; **postanowienie TK z 6.11.2019 r., SK 21/18**).

2.4.2. Naruszenie swobody działalności gospodarczej i zasady proporcjonalności (art. 20, art. 22 i art. 31 ust. 3 Konstytucji RP)

Swoboda działalności gospodarczej, stanowiąca fundament ustroju gospodarczego RP (art. 20 i art. 22 Konstytucji), może być ograniczana tylko w drodze ustawy i tylko ze względu na ważny interes publiczny. Każde takie ograniczenie musi jednak spełniać wymóg proporcjonalności, określony w **art. 31 ust. 3 Konstytucji RP**. Oznacza to, że zastosowany środek musi być przydatny, konieczny i proporcjonalny *sensu stricto*.

Całkowity zakaz stosowania sprzętu jest środkiem najdalej idącym, podczas gdy istnieją środki mniej dolegliwe, które mogłyby osiągnąć cel w postaci zapewnienia cyberbezpieczeństwa, takie jak certyfikacja, audyty czy wymóg dywersyfikacji dostawców, o których mowa w art. 103 ust. 2 tego samego aktu. Projektodawca nie wykazał, dlaczego środki z art. 103 ust. 2 CSA2 są niewystarczające. Wprowadzona regulacja jest zatem nieproporcjonalna i narusza zasadę racjonalności działań prawodawcy, dekodowaną z zasady demokratycznego państwa prawnego (art. 2 Konstytucji RP) (por. **wyrok TK z 25.05.2009 r., SK 54/08**).

2.4.3. Naruszenie prawa do sądu (art. 45 ust. 1 i art. 77 ust. 2 Konstytucji RP)

Projektowany mechanizm nie zapewnia podmiotom dotkniętym skutkami nakazu usunięcia komponentów ICT – czyli przedsiębiorcom – skutecznej drogi sądowej do kwestionowania decyzji Komisji. Forma aktu wykonawczego nie zapewnia im możliwości odwołania do sądu. Pozbawia ich to możliwości obrony swoich

praw, co stanowi rażące naruszenie konstytucyjnego prawa do sądu (**art. 45 ust. 1**) oraz zasady zakazującej zamykania drogi sądowej do dochodzenia naruszonych wolności lub praw (**art. 77 ust. 2**).

2.5. Podsumowanie rozważań

Podsumowując, należy stwierdzić, że projektowane w art. 103 ust. 1 i 7 i art. 110 CSA2 mechanizmy, w obecnym kształcie, poprzez ustanowienie instytucji wyłączenia bez odszkodowania oraz pozbawienie dotkniętych nim podmiotów skutecznej ochrony sądowej, w sposób rażący narusza fundamentalne prawa chronione Kartą Praw Podstawowych, w tym prawo własności, prawo do sądu oraz wolność prowadzenia działalności gospodarczej. **Na domiar złego**, w sytuacji gdy restrykcje te wynikają z **aktów wykonawczych Komisji Europejskiej**, wydawanych w **procedurze komitologicznej**, nie tylko bezpośrednio dotknięci nimi przedsiębiorcy nie mają prawa odwołania, ale również państwa członkowskie pozbawione są decydującego wpływu na ostateczny kształt zakazu użytkowania i nakazu usuwania komponentów ICT. Jest to szczególnie problematyczne, gdyż takie nakazy mogą mieć drastycznie zróżnicowany ciężar gospodarczy i społeczny dla poszczególnych państw członkowskich, w zależności od struktury ich rynków i dotychczasowych inwestycji.

Sytuacja, w której akt prawa wtórnego Unii Europejskiej jest niezgodny z Konstytucją RP, jest wysoce niepożądana. Może ona prowadzić do kolejnych kryzysów konstytucyjnych, podobnych do tych, które miały miejsce, gdy Trybunał Konstytucyjny orzekał o niezgodności prawa UE z Konstytucją, pomimo obowiązującej w porządku unijnym zasady pierwszeństwa. Konstytucja pozostaje najwyższym prawem Rzeczypospolitej Polskiej (art. 8 ust. 1 Konstytucji RP), a jej sprzeczność z prawem unijnym rodzi po stronie państwa polskiego obowiązek podjęcia działań zmierzających do zmiany prawa unijnego lub, w ostateczności, zmiany samej Konstytucji (por. **wyroki TK K 18/04 i SK 45/09**). Aby unikać takich sytuacji, wtórne prawo UE powinno być tworzone z poszanowaniem porządków konstytucyjnych państw członkowskich i chronionych przez nie wartości.

KIKE podkreśla, że Konstytucja pozostaje najwyższym prawem Rzeczypospolitej Polskiej (art. 8 ust. 1 Konstytucji RP), a polskie władze mają obowiązek sprzeciwiać się przyjmowaniu przez UE przepisów, które naruszają chronione w niej prawa i wolności obywatelskie, wyznaczające próg ochrony niepodlegający obniżeniu przez regulacje unijne (por. wyrok TK SK 45/09).

Mechanizmy przewidziane w art. 103 ust. 1 i 7 oraz art. 110 projektu CSA2, skutkujące przymusowym wycofaniem z użytku określonego sprzętu i oprogramowania, naruszają szereg fundamentalnych zasad konstytucyjnych i jako takie nie powinny się ostać.

3. Art. 99 ust. 3 jako zaprzeczenie idei pełnej harmonizacji (sprzeciw)

Zwracamy uwagę, że sam projekt CSA2 zawiera przepis, który może zniweczyć korzyści płynące z unifikacji, o których była mowa w pkt 1.1. niniejszego pisma. Mowa o **art. 99 ust. 3**, który przewiduje możliwość przyjęcia przez państwa członkowskie dalej idących rozwiązań mających na celu ustanowienie wyższego poziomu cyberbezpieczeństwa. Warunkiem jest, aby rozwiązania te były zgodne z obowiązkami państw członkowskich wynikającymi z prawa unijnego, jednak obowiązki te nie zostały w żaden sposób sprecyzowane. **Taka konstrukcja stanowi niebezpieczną i nieokreśloną furtkę, która w praktyce zaprzecza samej idei harmonizacji.** Zamiast tworzyć spójny i przewidywalny system na jednolitym rynku, przepis ten zachęca do wprowadzania krajowych specyfik, czyli do nadregulacji (*gold-plating*). Jest to praktyka, od której odradza sama Komisja Europejska w swoich wytycznych dotyczących lepszego stanowienia prawa (*Better Regulation Guidelines*), gdyż prowadzi ona do fragmentacji rynku wewnętrznego.

Wadliwość i niebezpieczeństwo płynące z art. 99 ust. 3 CSA2 objawiają się w szczególności w następujących aspektach:

- **Zaburzenie swobody przepływu towarów w świetle Traktatu o funkcjonowaniu Unii Europejskiej (TFUE):** Art. 99 ust. 3 dopuszcza sytuację, w której te same komponenty ICT będą w pełni legalne i dopuszczone do użytku w jednych państwach członkowskich, podczas gdy w innych zostaną objęte rygorystycznym zakazem. Taki stan rzeczy uderza bezpośrednio w jedną z fundamentalnych swobód

rynku wewnętrznego, zagwarantowaną w **art. 34 TFUE**, który zakazuje stosowania ograniczeń ilościowych w przywozie oraz wszelkich środków o skutku równoważnym. Zgodnie z ugruntowanym orzecnictwem Trybunału Sprawiedliwości UE (tzw. formuła Dassonville), za środek o skutku równoważnym uznaje się każdą regulację zdolną do wprowadzenia, bezpośrednio lub pośrednio, rzeczywiście lub potencjalnie, przeszkody w handlu wewnątrzwspólnotowym. Wprowadzanie przez poszczególne państwa członkowskie własnych, szerszych katalogów zakazanych komponentów ICT stanowi klasyczny przykład takiej bariery pozataryfowej. O ile **art. 36 TFUE** dopuszcza odstępstwa od tej swobody ze względów bezpieczeństwa publicznego, o tyle wyjątki te muszą być interpretowane ściśle. Działania państw członkowskich nie mogą stanowić środka arbitralnej dyskryminacji ani ukrytego ograniczenia w handlu między państwami członkowskimi. Pozostawienie w CSA2 tak szerokiej i niedookreślonej furtki stwarza ogromne ryzyko nadużywania klauzuli bezpieczeństwa do celów protekcyjnych, co doprowadzi do trwałej fragmentacji wspólnego rynku cyfrowego.

- **Niepewność regulacyjna dla przedsiębiorców:** Pozostawienie państwom członkowskim tak szerokiej swobody decyzyjnej rodzi fundamentalne pytanie: który dostawca jest faktycznie bezpieczny, a który nie? W sytuacji, gdy inny podmiot zostanie uznany za dostawcę wysokiego ryzyka (DWR) na poziomie UE, a zupełnie inny na poziomie krajowym, powstają drastycznie zróżnicowane warunki konkurencji. Przedsiębiorcy tracą tym samym możliwość opierania swoich długoterminowych strategii inwestycyjnych na przewidywalnym prawie.
- **Dyskryminacja krajowych MŚP i zachęta do arbitrażu technologicznego:** Zróżnicowanie zasad dopuszczalności sprzętu stawia w uprzywilejowanej pozycji międzynarodowe korporacje kosztem podmiotów z sektora MŚP. Przedsiębiorstwa o zasięgu międzynarodowym będą mogły swobodnie korzystać z arbitrażu technologicznego, płynnie przenosząc komponenty zakazane w jednym kraju do swoich oddziałów w państwach, gdzie takie restrykcje nie obowiązują. Z kolei polscy przedsiębiorcy krajowi, prowadzący działalność wyłącznie na jednym rynku, zostaną pozbawieni takiej możliwości, co w razie konieczności przymusowej wymiany sprzętu skaże ich na potężne i nieodwracalne straty.
- **Naruszenie zasady proporcjonalności:** Furtka kompetencyjna z art. 99 ust. 3 pozwala państwom członkowskim na wdrażanie środków najbardziej drastycznych – takich jak całkowity nakaz usunięcia sprzętu ze wszystkich warstw sieci – zamiast stosowania rozwiązań adekwatnych i mniej restrykcyjnych. Mechanizm DWR z założenia powinien służyć zarządzaniu ryzykiem (np. w łańcuchu dostaw), a nie fizycznej rozbiórce działającej infrastruktury. Właściwą reakcją powinna być dywersyfikacja dostawców lub ograniczenie wykorzystania sprzętu wyłącznie do funkcji krytycznych.

Warto zauważyć, że w innych aktach prawa unijnego, na przykład w dyrektywach usługowych, prawodawca precyzyjnie określa zakres swobody państw członkowskich, aby **zminimalizować ryzyko rozbieżności**. Projektowane w CSA2 przepisy niestety odchodzą od tej dobrej praktyki, pozostawiając zbyt mało określone szeroki i niedookreślony margines swobody regulacyjnej dla państw członkowskich, co **podważa główny cel regulacji, jakim jest stworzenie jednolitych ram prawnych dla cyberbezpieczeństwa w całej Unii**.

4. Art. 100 i nast. projektowanego aktu – obejście przepisów TFUE przez Komisję (sprzeciw)

KIKE protestuje przeciwko temu, aby Komisja Europejska uznawała kraj trzeci za stanowiący ryzyko dla łańcuchów dostaw ICT. Taka decyzja miałaby nieuchronne konsekwencje na arenie międzynarodowej dla wszystkich państw członkowskich. **Taka decyzja nie może być wydawana na podstawie aktu wydanego na podstawie art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (dalej: „TFUE”), który służy do zbliżania ustawodawstw pomiędzy państwami członkowskimi, a nie do prowadzenia polityki zagranicznej w relacjach z państwami trzecimi. Takie działania mają znamiona rozstrzygnięć, które powinny być podejmowane na podstawie art. 215 TFUE, czyli są to kompetencje Rady (państw członkowskich działających wspólnie, przy głosowaniu większością kwalifikowaną), a nie Komisji Europejskiej działającej *de facto* samodzielnie, w drodze aktów wykonawczych.**

4.1. Art. 114 TFUE jako niewłaściwa podstawa prawna

Zgodnie z utrwalonym orzecnictwem Trybunału Sprawiedliwości Unii Europejskiej, wybór podstawy prawnej dla aktu unijnego musi opierać się na obiektywnych czynnikach podlegających kontroli sądowej, a zwłaszcza na celu i treści aktu (tzw. test środka ciężkości, ang. *centre-of-gravity* approach). Jak wielokrotnie orzekał TSUE, akt powinien być oparty na podstawie prawnej odpowiadającej jego podstawowemu celowi (zob. m.in. C-155/91 Komisja p. Radzie, pkt 7; C-491/01 BAT, pkt 94).

Cel art. 114 TFUE: Przepis ten stanowi podstawę do przyjmowania środków mających na celu zbliżenie przepisów państw członkowskich, których celem jest ustanowienie i funkcjonowanie rynku wewnętrznego. Jak podkreślił Trybunał w fundamentalnym wyroku C-376/98 Niemcy p. Radzie (reklama tytoniu I), art. 114 TFUE nie tworzy ogólnego uprawnienia do regulowania rynku (pkt 83), a jedynie do przyjmowania środków, które mają rzeczywiście poprawić warunki jego funkcjonowania. Samo stwierdzenie różnic między porządkami krajowymi i abstrakcyjne ryzyko zakłóceń nie jest wystarczające (pkt 84). Wymagane jest, aby środek przyczyniał się do usunięcia rzeczywistych przeszkód w wykonywaniu swobód lub istotnych zakłóceń konkurencji (zob. także C-217/04 Zjednoczone Królestwo p. Parlamentowi i Radzie, pkt 42).

Cel art. 100 CSA2: Celem tego artykułu nie jest harmonizacja rynku, lecz stworzenie mechanizmu oceny i kwalifikacji państw trzecich jako stwarzających zagrożenie dla cyberbezpieczeństwa. Jest to w swojej istocie instrument polityki zewnętrznej i bezpieczeństwa, a nie regulacja rynku wewnętrznego. Jego głównym celem nie jest usuwanie barier handlowych, lecz ochrona Unii przed zagrożeniami o charakterze politycznym i dotyczącymi bezpieczeństwa, pochodzącymi spoza jej terytorium.

Skutki decyzji: Akt wykonawczy wydany na podstawie art. 100 CSA2 prowadzi do daleko idących restrykcji, w tym, jak wskazują dalsze przepisy projektu (np. art. 103), do zakazu stosowania określonego sprzętu i oprogramowania. Stanowi to środek ograniczający o charakterze sankcyjnym, a nie środek harmonizujący rynek.

Wybór podstawy prawnej nie może być podyktowany chęcią osiągnięcia innego celu niż ten, dla którego dana podstawa została przewidziana. Jeżeli podstawowym celem aktu nie jest usprawnienie rynku wewnętrznego, lecz np. ochrona zdrowia publicznego czy – jak w tym przypadku – bezpieczeństwa, sięganie po art. 114 TFUE jest nieuzasadnione.

4.2. Art. 215 TFUE jako właściwa podstawa prawna (*lex specialis*)

Znacznie bardziej adekwatną, a w istocie jedyną właściwą podstawą prawną dla środków przewidzianych w art. 100 projektu CSA2, jest art. 215 TFUE.

Przeznaczenie art. 215 TFUE: Zgodnie z jego treścią, stanowi on podstawę do przyjmowania środków ograniczających (sankcji) wobec państw trzecich, osób fizycznych lub prawnych. Jest to przepis szczególny (*lex specialis*) w stosunku do ogólnych norm, w tym także w stosunku do art. 114 TFUE, gdy powodem wprowadzenia ograniczeń są względy natury politycznej, wynikające z decyzji przyjętej w ramach Wspólnej Polityki Zagranicznej i Bezpieczeństwa (dalej: „WPZiB”). Kwalifikacja państwa trzeciego jako stwarzającego zagrożenie dla cyberbezpieczeństwa Unii jest bezsprzecznie decyzją o charakterze politycznym, mającą na celu ochronę fundamentalnych interesów bezpieczeństwa UE.

Gwarancje proceduralne: Procedura przewidziana w art. 215 TFUE jest dwuetapowa i zapewnia znacznie wyższy poziom legitymizacji i gwarancji proceduralnych dla tak doniosłych decyzji, ponieważ wymaga podjęcia jednomyślnej decyzji przez Radę w ramach WPZiB (zgodnie z art. 29 Traktatu o Unii Europejskiej). Następnie wymaga przyjęcia przez Radę, stanowiącą większość kwalifikowaną, niezbędnych środków wykonawczych na wspólny wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa oraz Komisji.

Zastosowanie art. 114 TFUE stanowi próbę obejścia rygorystycznej procedury przewidzianej dla nakładania środków ograniczających. Umożliwia Komisji Europejskiej, w ramach procedury komitologii, podjęcie decyzji o ogromnych skutkach gospodarczych i politycznych, która zgodnie z logiką traktatową powinna być zakotwiczona w ramach WPZiB i podlegać kontroli politycznej Rady na najwyższym szczeblu.

Podsumowując, wybór art. 114 TFUE jako podstawy prawnej dla art. 100 projektu CSA2 jest wadliwy, co znajduje potwierdzenie w ugruntowanym orzecnictwie TSUE dotyczącym wyboru podstawy prawnej.

Prowadzi do nieuprawnionego rozszerzenia kompetencji harmonizacyjnych na sferę polityki zewnętrznej i bezpieczeństwa. Prawidłową podstawą dla ustanowienia tak doniosłych w skutkach środków ograniczających wobec państw trzecich jest art. 215 TFUE, który jako *lex specialis* zapewnia odpowiednie gwarancje proceduralne i odzwierciedla polityczny charakter podejmowanych decyzji.

5. Aprobata dla katalogu zniuansowanych środków zaradczych z art. 103 ust. 2 (poparcie)

W kontekście projektowanych uprawnień Komisji Europejskiej do reagowania na zagrożenia związane z dostawcami wysokiego ryzyka, co do zasady należy pozytywnie ocenić instrumenty przewidziane w art. 103 ust. 2 lit. a)-d) oraz g) projektu rozporządzenia CSA2. Wskazane przepisy wprowadzają katalog zniuansowanych i stopniowalnych środków zaradczych, które pozwalają na adekwatną i proporcjonalną reakcję na zidentyfikowane ryzyko.

Stanowi to właściwą alternatywę dla najdalej idącego środka, jakim jest całkowity zakaz stosowania komponentów i nakaz ich usunięcia, który to środek, jak wskazano w innych częściach niniejszego stanowiska, budzi fundamentalne zastrzeżenia co do jego zgodności z zasadą proporcjonalności oraz prawem własności.

Możliwość zastosowania środków mniej restrykcyjnych, takich jak te przewidziane w literach a)-d) oraz g), pozwala na dostosowanie interwencji organu unijnego do wagi i charakteru naruszenia. Takie podejście jest w pełni zgodne z zasadą proporcjonalności (art. 5 ust. 4 Traktatu o Unii Europejskiej), która, jak wielokrotnie podkreślał Trybunał Sprawiedliwości UE, wymaga, aby środki prawne były zdatne do realizacji zamierzonego celu i nie wykraczały poza to, co jest konieczne do jego osiągnięcia (por. wyrok TS z 18.06.2015 r., C-508/13, Estonia przeciwko Parlamentowi i Radzie, pkt 28). Wyposażenie organów w takie instrumenty jak:

- wydawanie ostrzeżeń,
- nakazy zaprzestania naruszeń,
- przyjmowanie wiążących zobowiązań od dostawców,
- nakładanie obowiązku usunięcia określonych podatności,

jest zgodne z najlepszymi praktykami legislacyjnymi. Wykluczenie dostawcy z rynku powinno być środkiem ostatecznym (*ultima ratio*), stosowanym jedynie wówczas, gdy inne, mniej inwazyjne działania okażą się niewystarczające.

Należy jednakże jednoznacznie podkreślić, że aprobata ta nie obejmuje uprawnień wskazanych w lit. e) oraz f) ust. 2 ww. artykułu, które budzą zastrzeżenia z uwagi na ich nieproporcjonalny charakter.

W ocenie Izby, wyposażenie Komisji w elastyczny zestaw narzędzi interwencyjnych jest kierunkiem właściwym, umożliwiającym skuteczne zarządzanie cyberbezpieczeństwem bez nakładania na przedsiębiorców nieproporcjonalnych ciężarów ekonomicznych, które nieuchronnie wiązałyby się z obligatoryjnym stosowaniem jedynie najsurowszych restrykcji.

6. Naruszenie swobody działalności gospodarczej i fundamentalnych zasad proceduralnych (art. 105 CSA2) (sprzeciw)

KIKE stoi na stanowisku, że również przewidziany w art. 105 projektu system wniosków o zwolnienie z restrykcji jest wadliwy i prowadzi do nieproporcjonalnej ingerencji w swobodę działalności gospodarczej oraz narusza fundamentalne zasady proceduralne prawa unijnego i polskiego.

- **Odwroćenie ciężaru dowodu:** System ten w sposób niedopuszczalny odwraca ciężar dowodu. To nie instytucje Unii muszą udowodnić istnienie ryzyka, ale dostawca musi przedstawić „jasne dowody” i jednoznacznie udowodnić jego brak, aby uzyskać zwolnienie. Jest to sprzeczne z ogólną zasadą prawa unijnego, zgodnie z którą ciężar udowodnienia naruszenia spoczywa na organie, który je zarzuca (por. art. 2 Rozporządzenia 1/2003). Takie rozwiązanie narusza prawo do obrony i rzetelnego procesu (art. 47 KPP).

- **Brak uprawnień dla użytkowników:** Co jest kluczowe z perspektywy polskich przedsiębiorców, nie przyznano im żadnych uprawnień do samodzielnego inicjowania kontroli zasadności nałożonych na nich ograniczeń. Ich sytuacja prawna jest całkowicie uzależniona od skuteczności działania dostawcy, na którego działania nie mają żadnego wpływu. Jest to jawne naruszenie prawa do skutecznego środka prawnego (art. 47 KPP) oraz prawa do sądu (art. 45 Konstytucji RP).
- **Ograniczone przesłanki i dodatkowe bariery:** Przesłanki uzyskania zwolnienia są sformułowane w sposób bardzo wąski, a wszelkie koszty i opłaty związane z wnioskiem ponosi dostawca, co stanowi dodatkową barierę i narusza wolność prowadzenia działalności gospodarczej (art. 16 KPP oraz art. 20 i 22 Konstytucji RP).

Taka regulacja, zdaniem Izby, narusza zasadę ochrony praw nabytych oraz zasadę zaufania do państwa i stanowionego przez nie prawa (art. 2 Konstytucji RP).

Reasumując, w ocenie KIKE, przepisy CSA2, w szczególności w zakresie art. 103 ust. 1 i 7, art. 110 oraz art. 105, zawierają regulacje, które w sposób fundamentalny naruszają porządek prawny Rzeczypospolitej Polskiej oraz Unii Europejskiej. Stanowią one bezprecedensową ingerencję w prawa majątkowe i wolność gospodarczą, stwarzając poważne zagrożenie dla stabilności i konkurencyjności tysięcy polskich i europejskich przedsiębiorców.

W związku z powyższymi, fundamentalnymi wadami prawnymi, KIKE apeluje o podjęcie działań zmierzających do zmiany projektu CSA2 i w tym zakresie postuluje:

1. **Odrzucenie** przepisów art. 103 ust. 1 i 7, art. 110 oraz art. 105 w ich obecnym kształcie.
2. **Zapewnienie poszanowania praw człowieka, podstawowych zasad ustrojowych Unii Europejskiej i Rzeczypospolitej Polskiej, w tym zasady proporcjonalności**, poprzez poprzestanie na środkach ujętych w art. 103 ust. 2 CSA2, które powinny być nakładane w formie rozstrzygnięcia, które jest zaskarżalne do innego organu (sądu).
3. **Zagwarantowanie realnego prawa do sądu** dla wszystkich podmiotów dotkniętych regulacją, w tym prawa do zaskarżenia decyzji i przywrócenie klasycznego rozkładu ciężaru dowodu.

Z poważaniem



Karol Skupień

Prezes Zarządu KIKE