Do druku nr 1955

FEDERACJA
PRZEDSIĘBIORCÓW
POLSKICH

Al. Ujazdowskie 51 | 00-536 Warszawa | Tel.: +48 697 775 333

biuro@federacjaprzedsiebiorcow.pl
www.federacjaprzedsiebiorcow.pl

FPP/284/2025

Warszawa, 3 grudnia 2025 r.

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-III.0330.368.10.2025
Data wpływu 03.XII.25 r.

Pan
Włodzimierz Czarzasty
Marszałek Sejmu

Szanowny Panie Marszałku,

w związku ze skierowaniem do I czytania rządowego projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk sejmowy nr 1955, dalej jako: „**Projekt Ustawy**") przekazujemy poniżej uwagi Federacji Przedsiębiorców Polskich (dalej jako: „**FPP**").

Zwracamy się z prośbą o zlecenie ponownej analizy w celu modyfikacji propozycji zawartych Projekcie Ustawy w duchu zasady deregulacji „UE + 0". W szczególności postulujemy:

- ograniczenie zakresu regulacji do niezbędnej transpozycji **dyrektywy NIS2**[1] i zaleceń 5G Toolbox;
- stosowne odniesienie się do skoordynowanych ocen ryzyka przygotowywanych przez Komisję Europejską
- przywrócenie gwarancji proceduralnych dla przedsiębiorców oraz
- rezygnację z instrumentów naruszających kompetencje organów koncesyjnych i praw konstytucyjnych przedsiębiorców.

1. **Na wstępie chcielibyśmy zwrócić uwagę na niezwykle istotną wadą proceduralną Projektu Ustawy, jaką jest zaniechanie notyfikacji Komisji Europejskiej, której podlegają projekty aktów prawnych zawierających przepisy techniczne.**

   FPP zwracała uwagę na tę kwestię w ramach rządowego procesu legislacyjnego oraz przedstawiło opinię prawną (w załączniku), z której wynika, że Projekt Ustawy zawiera przepisy techniczne (w tym przede wszystkim przepisy w zakresie możliwości wykluczania komponentów ICT). Zgodnie z Dyrektywą TRIS (UE)2015/1535, ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, każdy akt zawierający tego rodzaju przepisy musi zostać zgłoszony Komisji

[1] 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 NIS 2); Dz. Urz. L 333 z 27.12.2022 r., s. 80.

Europejskiej. Doniesienia medialne wskazują, że Komisja już zwróciła uwagę na konieczność notyfikacji regulacji o cyberbezpieczeństwie.

Brak notyfikacji może skutkować uznaniem przepisów za niemające skutku wobec przedsiębiorców, co rodzi wysokie ryzyko roszczeń odszkodowawczych od Skarbu Państwa. Należy odnieść się także do zobowiązań międzynarodowych, które spoczywają na Polsce. **Dotyczy to notyfikacji w ramach w ramach Komitetu ds. barier technicznych w handlu (TBT) WTO, której projektodawca nie przewidział, a co może nieść ze sobą reperkusje w stosunkach z państwami należącymi do Światowej Organizacji Handlu.** Podobnie, przyjęcie przepisów umożliwiających wykluczanie określonych produktów z rynku przez wzgląd na państwo ich pochodzenia powoduje ryzyko arbitrażu podniesionego przez państwa, które zawarły z Polską (bezpośrednio lub za pośrednictwem UE) traktaty o inwestycjach (*Bilateral Investment Treaties*), a co dotyczyć może m.in. Izraela, Korei Południowej, Singapuru, Japonii, Wietnamu czy Chin, a więc państw, które są źródłami innowacyjnych technologii wykorzystywanych szeroko w wielu sektorach polskiej gospodarki. **W związku z tym wskazane jest co najmniej uzyskanie opinii Prokuratorii Generalnej RP i opinii sejmowego Biura Ekspertyz i Oceny Skutków Regulacji w zakresie ryzyk wywołanych przez brak stosowanych notyfikacji Projektu Ustawy.**

2. **Ponadto nasze obawy odnoszą się do przepisów dotyczących kontroli przedsiębiorców.**

Projekt przewiduje wyjątki od niektórych postanowień ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców[2]. W szczególności dotyczy to wyłączenia zakazu równoczesnego podejmowania i prowadzenia więcej niż jednej kontroli działalności przedsiębiorcy oraz braku obowiązku stworzenia protokołu kontroli w przypadku kontroli doraźnej przedsiębiorcy. Z perspektywy przedsiębiorcy wątpliwości budzi także projektowany art. 58 ust. 8 ustawy o krajowym systemie cyberbezpieczeństwa, który stanowi, że „w razie potrzeby", osoba prowadząca czynności kontrolne, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki do spraw kontroli zasadności zastrzeżeń do protokołu kontroli – zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu. Jak wskazywaliśmy w toku rządowego procesu legislacyjnego kontrola doraźna, możliwa do wszczęcia na podstawie tak nieprecyzyjnych przesłanek jak „sprawdzenie informacji zawartych w skargach i wnioskach", czy nawet na potrzeby wewnętrzne organu, bez obowiązku uprzedniego powiadomienia, stanowi nie tyle narzędzie weryfikacji, co instrument mogący doprowadzić do upadku wybranego przedsiębiorcę. W połączeniu z jednoinstancyjnym trybem wydawania decyzji nakazowych (art. 53 ust. 8), tworzy to ścieżkę eskalacji, gdzie przedsiębiorca jest systemowo pozbawiany możliwości skutecznej obrony na etapie administracyjnym, zanim organ sięgnie po najcięższe sankcje. Taki model jest sprzeczny nie tylko z zasadą demokratycznego państwa prawnego (art. 2 Konstytucji), ale również z wymogiem dyrektywy NIS2, która w art. 32 ust. 8 nakazuje w takich sytuacjach zapewnienie „rozsądnego czasu na przedstawienie uwag". Możliwość przeprowadzenia dodatkowych czynności kontrolnych powinna zostać ograniczona wyłącznie do przypadku, gdy kontrolowany zgłasza zastrzeżenia i sam wnosi o przeprowadzenie dodatkowych czynności kontrolnych, tak by nie być podwójnie „obciążanym" za skorzystanie z prawa zgłoszenia uwag do protokołu.

[2] Dz. U. z 2024 r. poz. 236 ze późn. zm.

3. **Niezwykle groźna z punktu widzenia polskich przedsiębiorców jest procedura wstrzymywania koncesji i zezwoleń.**

Wątpliwości budzi przyznanie organowi właściwemu do spraw cyberbezpieczeństwa kompetencji do ingerowania w wydane koncesje, zezwolenia i działalność, w tym działalność regulowaną, podmiotów kluczowych. Chodzi o projektowany art. 53 ust. 9 i n. ustawy o krajowym systemie cyberbezpieczeństwa, który przewiduje, że w razie niezastosowania się do nakazu podjęcia określonych czynności dotyczących obsługi incydentu lub niewykonania decyzji nakazującej podjęcie działań określonych w art. 53 ust. 5 pkt 2-8, organ ten może wstrzymać lub ograniczyć ww. koncesje, zezwolenia lub działalność. Skutków tego przepisu nie łagodzi fakt, iż złożenie skargi do sądu administracyjnego sprawia, że decyzja organu nie jest wykonywana, gdyż organ właściwy do spraw cyberbezpieczeństwa będzie mógł z dnia na dzień, bez wszczynania formalnego postępowania i bez uprzedzenia **wstrzymać funkcjonowanie danego przedsiębiorcy**. Co istotne decyzja jest wykonalna z dniem jej doręczenia aż do dnia złożenia skargi do sądu. Wskazać należy, że dotyczyć to może podmiotów zajmujących się dystrybucją produktów leczniczych, przewozami lotniczymi, czy zapewnianiem energii elektrycznej.

Dyrektywa NIS2 nie wymaga przyznania takich kompetencji organowi właściwemu do spraw cyberbezpieczeństwa – ma on mieć możliwość wystąpienia do sądu lub organu koncesyjnego o wstrzymanie koncesji. Dyrektywa NIS2 wyraźnie wskazuje, że kompetencja ta ma być spójna z krajowymi zasadami prawa i zapewniać odpowiednie prawa procesowe gwarantowane przez Kartę Praw Podstawowych i Europejską Konwencję Praw Człowieka, podczas gdy Projekt Ustawy wprowadza asystemową, wyjątkową instytucję wyposażając „organ właściwy do spraw cyberbezpieczeństwa" w qausi-sądową władzę.

4. **Należy zwrócić także na uwagę na nadregulację związaną z procedurą uznania za dostawcę wysokiego ryzyka, która nie tylko narusza podstawowe prawa konstytucyjne, ale i nieprawidłowo wdraża podstawowy dokument będący zaleceniami, a nie wiążącym prawem, tj. 5G Toolbox.**

Procedura ta pozwala Ministrowi Cyfryzacji, w oparciu o wysoce uznaniowe kryteria wykluczanie określonych elementów ICT z rynku (a więc każdego elementu podłączonego do Internetu) i nakazuje wycofanie takiego z użycia przez podmioty objęte ustawą. W ramach tych procedur Minister Cyfryzacji będzie mógł w drodze decyzji administracyjnej uznać dostawcę określonego sprzętu lub oprogramowania za „dostawcę wysokiego ryzyka" (projektowany art. 67b ust. 15) która będzie miała rygor natychmiastowej wykonalności *ex lege* (projektowany art. 67b ust. 18).

Skutkiem decyzji o uznaniu podmiotu za dostawcę wysokiego ryzyka będzie nakaz pozbycia się przez przedsiębiorców i inne instytucje objęte ustawą tych sprzętów i oprogramowania (projektowany art. 67c ust. 1). Od decyzji przysługuje skarga do WSA, niemniej projektodawca wykluczył możliwość przeprowadzenia rozprawy (projektowany art. 67e ust. 1), a wyrok z pełnym uzasadnieniem ma dostać tylko minister (projektowany art. 67e ust. 2), natomiast skarżący jedynie uzasadnienie w okrojonej wersji. Analogicznie uregulowana jest procedura dot. polecenia zabezpieczającego. Co więcej, WSA w obu przypadkach bada decyzję tylko pod kątem jej legalności, co przy ogólnych i nieokreślonych przesłankach uniemożliwia realizację zasady skutecznej ochrony sądowej. Model ten generuje istotne wątpliwości konstytucyjne podnoszone m.in. przez Rzecznika Praw Obywatelskich. Istotnie ingeruje w działalność gospodarczą podmiotów ważnych i kluczowych, stanowiąc swoiste wywłaszczenie, co jest niedopuszczalne, o ile nie został ogłoszony jeden ze stanów nadzwyczajnych(art. 20 w zw. z art. 22, z art. 31 ust. 3 oraz z art. 64 Konstytucji). **Tym samym procedura ta stanowi obejście Rozdziału IX Konstytucji i naruszenie zasady proporcjonalności**. W świetle powyższych, fundamentalnych

z punktu widzenia konstytucyjnych problemów, niezwykle niepokojący jest brak udziału dostawcy, którego status stanowi przedmiot postepowania, wraz z natychmiastową wykonalnością decyzji uniemożliwia czynny udział w postępowaniu.

Co więcej, **procedura ta w swoich skutkach przypomina represje karne, tj. środki karne w postaci zakazu wykonywania określonej działalności, w związku z tym powinna być stosowana przede wszystkim sądowo lub pod realną w znaczeniu Europejskiej Konwencji Praw Człowieka, kontrolą stosowną, zapełniająca pełną jurysdykcję, czego odwołanie do WSA nie zapewnia** (art. 45 ust. 1 w zw. z art. 78 i art. 61 Konstytucji).

5. **Błędna jest także sama konstrukcja oceny dostawcy jako dostawcy wysokiego ryzyka**

   Przewidziana w Projekcie Ustawy sama konstrukcja oceny dostawcy jako dostawcy wysokiego ryzyka nie uwzględnienia bowiem unijnych skoordynowanych ocen ryzyka jako punktu odniesienia do oceny produktów, usług i procesów ICT uznawanych za krytyczne i pomijanie przy ocenie kraju pochodzenia sprzętu ryzyka o charakterze stricte technicznym.

   Opisany mechanizm DWR dotyczy zgodnie z zaleceniami 5G Toolbox tylko sieci 5G. Projekt Ustawy rozszerza go jednak na wszystkie produkty, usługi i procesy ICT wykorzystywane w 18 sektorach, a więc daleko poza te zalecenia.

   Co więcej, wprowadzone procedury wycofywania komponentów ICT koliduje z zasadami wynikającymi z rozporządzenia UE 2022/2554 (Akt o cyberodpodrności CRA)[3]. CRA zawiera odrębną, unijną procedurę wycofywania z rynku produktów cyfrowych niespełniających wymagań bezpieczeństwa. **Jest ona dokładnie opisana i stopniowa, przewidując nie tylko ogólne domniemanie zgodności certyfikowanych produktów, ale na poszczególnych etapach danej procedury traktec wycofanie produktów jako ostateczność (*ultima ratio*).**

Z uwagi na powyższe zwracamy się z prośbą podjęcie działań zmierzających do zapewnienia, że w procesie legislacyjnym dotyczącym Projektu Ustawy zostaną uwzględnione postulaty deregulacyjne, a przede wszystkim opinie i propozycje ekspertów branżowych reprezentujących organizację zrzeszające polskich przedsiębiorców.

Załącznik:

Opinia prawna w sprawie obowiązku notyfikacji projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Prof. P. Bogdanowicz)

Z poważaniem,

Marek Kowalski
Przewodniczący
Federacji Przedsiębiorców Polskich

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011; Dz. Urz. L 333 z 27.12.2022, s. 1.

Warszawa, 14 czerwca 2023 r.
(zaktualizowana 5 lipca 2023 r. oraz 10 maja 2024 r.)

Prof. ucz. dr hab. Piotr Bogdanowicz
Wydział Prawa i Administracji
Uniwersytet Warszawski

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

I. Wprowadzenie

1. Przedmiotem niniejszej opinii prawnej ("**Opinia**") jest ocena obowiązku notyfikacji projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[1] ("**Projekt Ustawy**"), w zakresie dotyczącym uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, zgodnie z dyrektywą (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego ("**Dyrektywa 2015/1535**").
2. Na mocy art. 67b ust. 1 Projektu Ustawy, minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania[2], które są wykorzystywane przez:

[1] Najnowsza wersja z dnia 23 kwietnia 2024 r., dostępna na stronie internetowej: https://legislacja.rcl.gov.pl/projekt/12384504/katalog/13055195#13055195.

[2] Pod którym należy rozumieć dostawcę procesów ICT, produktów ICT lub usług ICT w rozumieniu, odpowiednio, art. 1 pkt 2 lit. j) ppkt 11h), 11i) oraz 11j) Projektu.

a. podmioty kluczowe lub podmioty ważne, z wyłączeniem podsektora komunikacji elektronicznej lub
b. przedsiębiorców telekomunikacyjnych, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych

– za dostawcę wysokiego ryzyka.

3. Minister wydaje decyzję o uznaniu dostawcy za dostawcę wysokiego ryzyka, w przypadku stwierdzenia, że dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi (art. 67b ust. 15). Decyzja zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka (art. 67b ust. 15).
4. Zgodnie z art. 67c ust. 1 Projektu, w przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o których mowa w art. 67b ust. 1: nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka oraz wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15. Z kolei przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.
5. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 pkt 2, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeżeli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń (art.

67c ust. 3 Projektu). Ponadto, podmioty, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nie mogą nabywać sprzętu, oprogramowania i usług określonych w decyzji (art. 67c ust. 4 Projektu). W przypadku, w którym podmioty te nabyły już produkt ICT, usługę ICT lub proces ICT mogą z nich korzystać nie dłużej niż 7 lat (5 lat – w przypadku wykorzystywania ich do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy) (art. 67c ust. 5).

6. Zgodnie z uzasadnieniem Projektu Ustawy, "nie zawiera [on] przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i w związku z tym nie podlega procedurze notyfikacji."[3]. Mając na uwadze, że rozporządzenie to stanowi transpozycję do prawa polskiego Dyrektywy 2015/1535 w Opinii skupiam się na ocenie obowiązku notyfikacji Projektu w świetle Dyrektywy 2015/1535 właśnie.
7. Rozpoczynam od przedstawienia konkluzji.

II. Konkluzje

1. **Przepisy art. 67c Projektu w zw. z art. 67b Projektu Ustawy mieszczą się w kategorii zakazujących przepisów technicznych, przez które należy rozumieć przepisy zakazujące produkcji, przywozu, wprowadzania do obrotu lub stosowania produktu lub zakazujące świadczenia bądź korzystania z usługi lub ustanawiania dostawcy usług, a tym samym stanowią przepisy techniczne w rozumieniu Dyrektywy 2015/1535.**
2. **W związku z powyższym Projekt Ustawy podlega przekazaniu (notyfikacji) Komisji Europejskiej na podstawie art. 5 ust. 1 Dyrektywy 2015/1535.**
3. **Podobne projekty przepisów uchwalone w innych państwach członkowskich (Irlandia, Hiszpania) zostały przekazane (notyfikowane) Komisji Europejskiej.**
4. **Zgodnie z art. 6 ust. 1 Dyrektywy 2015/1535 Rzeczpospolita Polska powinna odroczyć przyjęcie przepisów technicznych co najmniej o 3**

[3] Przy czym niektóre z wcześniejszych wersji Projektu Ustawy były przewidziane do notyfikacji.

miesiące począwszy od daty otrzymania przez Komisję zgłoszenia (notyfikacji) Projektu Ustawy.

III. Ocena obowiązku notyfikacji

Zakres przedmiotowy Dyrektywy 2015/1535

1. Zgodnie z art. 5 ust. 1 Dyrektywy 2015/1535, państwa członkowskie są, co do zasady, obowiązane do niezwłocznego przekazania Komisji Europejskiej ("**Komisja**") wszelkich projektów przepisów technicznych. Jak wskazał Trybunał Sprawiedliwości Unii Europejskiej ("**Trybunał**" lub "**TSUE**"), taka notyfikacja ma na celu ochronę – za pomocą kontroli prewencyjnej – swobodnego przepływu towarów, który jest jedną z podstaw Unii Europejskiej, a kontrola ta jest przydatna ze względu na to, iż przepisy techniczne objęte tą dyrektywą mogą stanowić przeszkody w handlu między państwami członkowskimi, które to przeszkody dopuszczalne są jedynie wówczas, gdy są one niezbędne, aby spełnić wymogi nadrzędne, których przestrzeganie leży w interesie ogólnym [4]. W konsekwencji, Komisja musi mieć dostęp do niezbędnych informacji przed przyjęciem przepisów technicznych[5].
2. Obowiązek notyfikacji nie ma charakteru bezwzględnego. Z art. 1 ust. 2-6 Dyrektywy 2015/1535 wynika, że nie ma ona zastosowania do:
    a. usług radiowej emisji dźwięku (art. 1 ust. 2 lit. a);
    b. usług rozpowszechniania telewizyjnego objętych zakresem art. 1 ust. 1 lit. e) dyrektywy Parlamentu Europejskiego i Rady 2010/13/UE (art. 1 ust. 2 lit. b);
    c. zasad odnoszących się do zagadnień objętych przepisami Unii w dziedzinie usług telekomunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2002/21/WE ("**Dyrektywa 2002/21**") (art. 1 ust. 3);

---

[4] Por. wyroki: z dnia 8 września 2005 r. w sprawie C-303/04, *Lidl Italia*, pkt 22; z dnia 15 kwietnia 2010 r. w sprawie C-433/05, *Sandström*, pkt 42; z dnia 9 czerwca 2011 r. w sprawie C-361/10 *Intercommunale Intermosane i Fédération de l'industrie et du gaz*, pkt 10 oraz z dnia 31 stycznia 2013 r. w sprawie C-26/11, *Belgische Petroleum*, pkt 49.

[5] Motyw 5 preambuły Dyrektywy 2015/1535.

d. zasad odnoszących się do zagadnień objętych przepisami Unii w dziedzinie usług finansowych, których przykładowy wykaz został zawarty w załączniku II do Dyrektywy 2015/1535 (art. 1 ust. 4);
e. zasad ustanowionych przez lub dla rynków regulowanych w rozumieniu dyrektywy Parlamentu Europejskiego i Rady 2004/39/WE bądź przez lub dla innych rynków lub organów realizujących operacje rozrachunkowe lub funkcje rozliczeniowe dla tych rynków[6] (art. 1 ust. 5) oraz
f. tych środków, które państwa członkowskie uznają za niezbędne, na mocy Traktatów, dla ochrony osób, w szczególności pracowników, podczas stosowania produktów, pod warunkiem że środki te pozostają bez wpływu na produkt (art. 1 ust. 6).

3. Ze względu na przedmiot Opinii, nie ma wątpliwości, że wyłączenia wskazane w art. 1 ust. 2, 4-6 Dyrektywy 2015/1535 nie mają znaczenia z perspektywy dalszej analizy. Przed przystąpieniem do oceny przepisów art. 67c w zw. z art. 67a Projektu Ustawy jako przepisów technicznych, należy jednak przeanalizować czy w związku z wyłączeniem, o którym mowa w art. 1 ust. 3 Dyrektywa 2015/1535 może w ogóle znaleźć zastosowanie w sprawie.
4. Artykuł 1 ust. 3 literalnie odwołuje się do Dyrektywy 2002/21. Na podstawie art. 125 akapit pierwszy dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej ("**Dyrektywa 2018/1972**"), Dyrektywa 2002/21 została uchylona z mocą od dnia 21 grudnia 2020 r. Odesłanie do uchylonej Dyrektywy 2002/21, zgodnie z art. 125 akapit trzeci Dyrektywy 2018/1972, należy odczytywać jako odesłanie do Dyrektywy 2018/1972.
5. Zgodnie z art. 1 ust. 1, Dyrektywa 2018/1972 ustanawia zharmonizowane ramy prawne regulujące sieci łączności elektronicznej, usługi łączności elektronicznej, urządzenia i usługi towarzyszące i niektóre aspekty urządzeń końcowych. Określa ona zadania krajowych organów regulacyjnych i, w stosownych przypadkach, innych właściwych organów oraz zbiór procedur w celu zapewnienia zharmonizowanego stosowania ram prawnych w obrębie Unii. **Gdyby więc przyjąć, że projektowane regulacje dotyczące**

[6] Z wyjątkiem art. 5 ust. 3 Dyrektywy 2015/1535.

postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka mieszczą się w zakresie przedmiotowym Dyrektywy 2018/1972, wskazanym w ww. art. 1 ust. 1, mogłoby to oznaczać, że regulacje te są wyłączone z obowiązku notyfikacji na mocy art. 1 ust. 3 Dyrektywy 2015/1535 bez konieczności badania czy mamy do czynienia w analizowanej sprawie z przepisami technicznymi, czy nie. Tak moim zdaniem jednak nie jest. Wynika to z następujących względów.

6. **Po pierwsze**, wbrew literalnej treści art. 1 ust. 3 Dyrektywy 2015/1535, Dyrektywa 2018/1972 stanowi, że niektóre usługi łączności elektronicznej objęte tą dyrektywą mogą również wchodzić w zakres definicji "usługi społeczeństwa informacyjnego" zawartej w art. 1 Dyrektywy 2015/1535. Zgodnie z motywem 10 preambuły Dyrektywy 2018/1972, przepisy Dyrektywy 2015/1535 regulujące usługi społeczeństwa informacyjnego mają zastosowanie do wspomnianych usług łączności elektronicznej "w zakresie nieobjętym bardziej szczegółowymi przepisami mającymi zastosowanie do usług łączności elektronicznej wynikającymi z niniejszej dyrektywy lub innych aktów prawnych Unii". Jak się wydaje, intencją prawodawcy unijnego było zatem wskazanie, że procedura notyfikacji określona w Dyrektywie 2015/1535 może znaleźć zastosowanie (przynajmniej) do usług łączności elektronicznej, o których mowa w Dyrektywie 2018/1972, chyba że przepisy prawa Unii Europejskiej, w tym Dyrektywy 2018/1972, stanowią inaczej (zawierają bardziej szczegółowe regulacje). Wykładnię tę zdają się potwierdzać inne motywy preambuły[7] oraz przepisy[8] Dyrektywy 2018/1972, wprost odwołujące się do Dyrektywy 2015/1535 (np. w zakresie środków dotyczących interoperacyjności konsumenckich odbiorników radiowych czy regulacji technicznych dotyczące pól elektromagnetycznych).
7. **Po drugie**, Dyrektywa 2018/1972 nie zawiera regulacji dotyczących kwestii profilu ryzyka dostawców w kontekście bezpieczeństwa dostarczanego sprzętu czy oprogramowania. Dyrektywa 2018/1972 reguluje, co prawda, w art. 40 i 41 kwestie bezpieczeństwa sieci i usług[9]. Zgodnie z tymi przepisami, państwa

[7] Por. motywy 80, 93, 191 i 304.

[8] Por. art. 39 i 58.

[9] Przynajmniej do 18 października 2024 r., w związku z uchyleniem obu przepisów przez art. 43 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie

członkowskie są obowiązane zapewnić, aby dostawcy udostępniający publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowały właściwe i proporcjonalne środki techniczne i organizacyjne w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Środki te muszą zapewniać poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii[10]. W związku z powyższym państwa członkowskie są również obowiązane zapewnić, aby podmioty udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej powiadamiały bez zbędnej zwłoki właściwy organ o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług[11]. Nie ulega jednak wątpliwości, że art. 67c czy art. 67b Projektu Ustawy dotyczą zupełnie innych sytuacji niż określone w art. 40 i 41 Dyrektywy 2018/1972, zaczynając od zakresu podmiotowego (dostawcy sprzętu czy oprogramowania vs dostawcy udostępniający publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej), a kończąc na przedmiocie regulacji (kwestia incydentów związanych z bezpieczeństwem i mających wpływ na funkcjonowanie sieci lub usług). Potwierdza to uzasadnienie jednej z wcześniejszych wersji Projektu Ustawy, z którego wprost wynikało, że transpozycję właściwych przepisów art. 40 i 41 Dyrektywy 2018/1972 stanowić miały zupełnie inne przepisy niż regulacje zawarte obecnie w art. 67c czy art. 67b Projektu Ustawy.

8. Podsumowując, **prawodawca unijny nie wyłączył z zakresu zastosowania Dyrektywy 2015/1535 przepisów dotyczących uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka**.
9. Zgodnie z art. 5 ust. 1 Dyrektywy 2015/1535, państwa członkowskie nie są jednak obowiązane do przekazania (notyfikacji) przepisów technicznych, które

---

środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (**"Dyrektywa NIS 2"**). Projekt Ustawy wdraża do polskiego porządku prawnego właśnie Dyrektywę NIS 2 – do zagadnienia tego wrócę jeszcze w dalszej części Opinii.

[10] Por. art. 40 ust. 1 Dyrektywy 2018/1972.

[11] Por. art. 40 ust. 2 Dyrektywy 2018/1972. Na mocy art. 41 Dyrektywy 2018/1972 właściwe organy państw członkowskich powinny być również uprawnione do wydawania wiążących instrukcji podmiotom udostępniającym publiczne sieci łączności elektronicznej lub świadczącym publicznie dostępne usługi łączności elektronicznej.

w pełni stanowią transpozycję normy europejskiej[12]. Należy zatem ocenić czy Projekt Ustawy w zakresie dotyczącym uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka stanowi transpozycję przepisów prawa unijnego do porządku krajowego, która mogłaby zwolnić Rzeczpospolitą Polskę z ewentualnego obowiązku notyfikacji Projektu Ustawy do Komisji.

10. **Moim zdaniem, Projekt Ustawy w zakresie dotyczącym uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka nie stanowi transpozycji przepisów prawa unijnego do polskiego porządku prawnego.**
11. Jak wskazano powyżej, Projekt Ustawy wdraża do polskiego porządku prawnego Dyrektywę NIS2. Nie ulega wątpliwości, że celem Dyrektywy NIS2 jest ustanowienie środków mających na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego (art. 1 ust. 1 Dyrektywy NIS 2). W związku z tym Dyrektywa NIS 2 określa m.in. obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów spoczywające na podmiotach, do których stosuje się Dyrektywę NIS 2 (art. 1 ust. 2 lit. a) i b)). **Dyrektywa NIS 2 w żadnym miejscu nie zawiera jednak przepisów, które dotyczyłyby uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, a w konsekwencji zakazywałyby wprowadzania do użytkowania określonych procesów, produktów czy usług albo nakazywałyby wycofania ich z użytkowania.**
12. Powyższe nie oznacza, że Dyrektywa NIS 2 uniemożliwia państwom członkowskim przyjęcie czy utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa. Przeciwnie, art. 5 Dyrektywy NIS 2, podkreślając minimalny poziom harmonizacji objętej dyrektywą, wskazuje, że państwa członkowskie mogą przyjmować czy utrzymywać w mocy określone przepisy, pod warunkiem jednak, "że takie przepisy są spójne z obowiązkami państw członkowskich, ustanowionymi w prawie Unii". Współgra to z celem Dyrektywy 2015/1535 – notyfikacja przepisów technicznych ma bowiem przecież na celu ochronę prawa unijnego w postaci swobodnego przepływu towarów.

[12] W takim przypadku wystarczająca jest informacja dotycząca odpowiedniej normy.

13. Potwierdza to wprost uzasadnienie Projektu Ustawy. Po pierwsze, w części dotyczącej dostawcy wysokiego ryzyka[13], w uzasadnieniu nie odesłano (ani nawet nie nawiązano w żaden sposób) do Dyrektywy NIS 2. Innymi słowy, prawodawca jest świadomy, że art. 67c czy art. 67b nie stanowią transpozycji do prawa polskiego przepisów Dyrektywy NIS 2. Po drugie, w uzasadnieniu wskazano, że "wprowadzenie zmian do ustawy o KSC [krajowym systemie cyberbezpieczeństwa] jest elementem działań na rzecz wdrożenia zaleceń z 5G Toolbox w Polsce" [14] (podkreślenie własne), a więc dokumentu opracowanego w styczniu 2020 r. przez Grupę Współpracy NIS. Nie ulega wątpliwości, że dokument ten nie mieści się w katalogu wiążących źródeł prawa pochodnego, o których mowa w art. 288 Traktatu o funkcjonowaniu Unii Europejskiej[15] i objętych obowiązkiem transpozycji do prawa krajowego.

14. **Należy ponadto zwrócić uwagę na notyfikacje dokonywane w ostatnich latach przez inne państwa członkowskie. Przykładowo, pod koniec 2022 r. Irlandia dokonała notyfikacji przepisów, których celem było wprowadzenie do prawa irlandzkiego definicji sprzedawcy wysokiego ryzyka** i przyznanie właściwemu ministrowi "pewnych uprawnień umożliwiających zarządzanie ryzykiem związanym z sieciami łączności elektronicznej, zgodnie z zaleceniami unijnego zestawu narzędzi bezpieczeństwa 5G"[16]. Wprost z tego wynika, że władze irlandzkie brały pod uwagę zalecenia z 5G Toolbox, ale nie oceniały, że stanowią one jakąkolwiek przeszkodę dla notyfikacji projektowanych przepisów na podstawie Dyrektywy 2015/1535. **Podobnie postąpiła pod koniec 2023 r. Hiszpania**, notyfikując projekt dekretu królewskiego zatwierdzającego krajowy system bezpieczeństwa sieci i usług 5G, który również odwoływał się do "dostawców wysokiego ryzyka", "uwzględniając zalecenie Komisji Europejskiej (UE) 2019/534 z dnia 26 marca 2019 r. cyberbezpieczeństwo sieci 5G, a także zalecenia zawarte w komunikacie Komisji Europejskiej z dnia 29 stycznia 2020 r. bezpieczne wprowadzanie sieci 5G w UE – wdrażanie

---

[13] Uzasadnienie Projektu Ustawy, pkt 2.22.2, s. 58 i n.

[14] Uzasadnienie Projektu Ustawy, s. 6.

[15] W katalogu tym znajdują się rozporządzenia, dyrektywy oraz decyzje.

[16] Notyfikacja nr 2022/0850/IRL z 9 grudnia 2022 r., dostępna tutaj: https://technical-regulation-information-system.ec.europa.eu/pl/notification/23272.

unijnego zestawu narzędzi (COM/2020/50 final) skierowanym do państw członkowskich na temat stosowania tego zestawu narzędzi."[17].

15. W związku z powyższym należy ocenić czy art. 67c w zw. z art. 67b Projektu Ustawy stanowią przepisy techniczne.

Ocena przepisów Projektu jako przepisów technicznych w rozumieniu Dyrektywy 2015/1535

16. Zgodnie z art. 1 ust. 1 lit. f) Dyrektywy 2015/1535 "przepisy techniczne" oznaczają specyfikacje techniczne i inne wymagania bądź zasady dotyczące usług, włącznie z odpowiednimi przepisami administracyjnymi, których przestrzeganie jest obowiązkowe, *de jure* lub *de facto*, w przypadku wprowadzenia do obrotu, świadczenia usługi, ustanowienia operatora usług lub korzystania w państwie członkowskim lub na przeważającej jego części, jak również przepisy ustawowe, wykonawcze i administracyjne państw członkowskich, z wyjątkiem określonych w art. 7, zakazujące produkcji, przywozu, wprowadzania do obrotu lub stosowania produktu lub zakazujące świadczenia bądź korzystania z usługi lub ustanawiania dostawcy usług.
17. Jak słusznie wskazuje się w literaturze przedmiotu, przepis techniczny może mieć zatem postać jednej z czterech kategorii:
    a. specyfikacji technicznej;
    b. innych wymagań;
    c. zasad dotyczących usług oraz
    d. **zakazujących przepisów technicznych, przez które należy rozumieć przepisy zakazujące produkcji, przywozu, wprowadzania do obrotu lub stosowania produktu lub zakazujące świadczenia bądź korzystania z usługi lub ustanawiania dostawcy usług**[18].
18. Mając na uwadze, że Projekt Ustawy, w przypadku jego przyjęcia, miałby formę przepisów ustawowych w rozumieniu art. 1 ust. 1 lit. f) Dyrektywy 2015/1535, należy ocenić czy art. 67c w zw. z art. 67b Projektu Ustawy mogą być uznane

---

[17] Notyfikacja nr 2023/0761/ES z 29 grudnia 2023 r., dostępna tutaj: https://technical-regulation-information-system.ec.europa.eu/pl/notification/25285.

[18] Zob. R. Maruszkin, *Poprawność procesu ustawodawczego ustawy o grach hazardowych w kontekście dyrektywy 2015/1535/UE ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego* [w:] M. Taborowski (red.), *Skutki braku notyfikacji przepisów technicznych ustawy o grach hazardowych dla wymiaru sprawiedliwości Rzeczypospolitej Polskiej*, Warszawa 2016, s. 101-102.

za "przepisy zakazujące produkcji, przywozu, wprowadzania do obrotu lub stosowania produktu lub zakazujące świadczenia bądź korzystania z usługi lub ustanawiania dostawcy usług". W ocenie Trybunału, w związku z tym, że ta kategoria przepisów technicznych dotyczy w szczególności zakazu używania, chodzi tu o przepisy, których zakres wyraźnie wykracza poza zacieśnienie możliwości używania spornego produktu do pewnych możliwych zastosowań, a zatem które nie sprowadzają się do zwykłego ograniczenia używania tego produktu i pozostawiają miejsce jedynie na marginalne zastosowanie danego produktu w stosunku do tego, którego można by rozsądnie oczekiwać[19].

19. **Uważam, że art. 67c Projektu w zw. z art. 67b Projektu Ustawy mieszczą się w kategorii zakazujących przepisów technicznych, tj. przepisów zakazujących produkcji, przywozu, wprowadzania do obrotu lub stosowania produktu lub zakazujących świadczenia bądź korzystania z usługi lub ustanawiania dostawcy usług. Tym samym przepisy te stanowią przepisy techniczne w rozumieniu Dyrektywy 2015/1535.** Konsekwencją wydania decyzji o uznaniu dostawy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka jest bowiem zakaz wprowadzania do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka. Zakaz ten jest równoznaczny z zakazem wprowadzania do obrotu, o którym mowa w art. 1 ust. 1 lit. f) Dyrektywy 2015/1535. Podobnie należy traktować zakaz nabywania sprzętu, oprogramowania i usług określonych w decyzji przez podmioty obowiązane do stosowania Prawa zamówień publicznych – w tym przypadku wiązać się to może również z przewidzianym w Dyrektywie 2015/1535 zakazem przywozu takiego sprzętu czy oprogramowania. Obowiązek wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji jest z kolei równoznaczny z zakazem stosowania produktu, świadczenia i korzystania z usługi (po upływie tego okresu).

---

[19] Por. wyrok z dnia 21 kwietnia 2005 r. w sprawie C-267/03, *Lindberg*, pkt 76 i 77.

20. Wydaje się natomiast, że dopuszczenie użytkowania dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w okresie tych 7 lat, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeżeli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń, może spełniać określony przez Trybunał test "marginalności". Dokonywanie napraw, przeprowadzane modernizacje czy aktualizacje mogą bowiem umożliwiać w miarę niezakłócone zastosowanie danego produktu.
21. **W związku z powyższym Projekt Ustawy powinien podlegać przekazaniu (notyfikacji) Komisji na podstawie art. 5 ust. 1 Dyrektywy 2015/1535.** Co istotne, jak wynika z orzecznictwa TSUE, obowiązek notyfikacji obejmuje cały tekst projektu aktu prawnego zawierającego przepisy techniczne, tj. łącznie z przepisami, które w ocenie państwa członkowskiego nie mają takiego charakteru. Chodzi bowiem o to, aby Komisja miała możliwość dokonania całościowej oceny projektu z punktu widzenia kwalifikacji zawartych w nim regulacji jako przepisów technicznych[20].
22. **Zgodnie z art. 6 ust. 1 Dyrektywy 2015/1535 Rzeczpospolita Polska powinna odroczyć przyjęcie przepisów technicznych co najmniej o 3 miesiące począwszy od daty otrzymania przez Komisję zgłoszenia (notyfikacji) Projektu Ustawy.** Biorąc pod uwagę, że obecny Projekt Ustawy stanowi którąś już wersję regulacji mających na celu zmianę przepisów o krajowym systemie cyberbezpieczeństwa i prace legislacyjne trwają już ponad dwa lata nie widzę podstaw do zastosowania przez Rzeczpospolitą Polskę art. 6 ust. 7 Dyrektywy 2015/1535, zwalniającego z obowiązku odroczenia przyjęcia przepisów "z naglących powodów, spowodowanych przez poważne i nieprzewidziane okoliczności odnoszące się [...] bezpieczeństwa publicznego [kiedy] państwo członkowskie jest zobowiązane przygotować przepisy techniczne w bardzo krótkim czasie, w celu ich natychmiastowego przyjęcia i wprowadzenia w życie bez możliwości jakichkolwiek konsultacji".

[20] Wyrok z dnia 16 września 1997 r. w sprawie C-279/94, *Komisja przeciwko Włochom*, pkt 40 i 41.

Konsekwencje braku notyfikacji

23. Z utrwalonego orzecznictwa TSUE wynika, że brak notyfikacji przepisów technicznych powoduje przede wszystkim, że przepisy te już po ich przyjęciu (uchwaleniu) nie mogą być stosowane, a zwłaszcza powoływane względem jednostek[21].
24. Brak notyfikacji może również skutkować wszczęciem przez Komisję Europejską postępowania o uchybienie jednemu z zobowiązań, które ciążą na państwie członkowskim na mocy Traktatów w trybie art. 258 Traktatu o funkcjonowaniu Unii Europejskiej.

IV. Zastrzeżenia

1. Nie wyrażam żadnej opinii co do faktów.
2. Opinia dotyczy tylko kwestii wskazanej powyżej w punkcie I.2.
3. Opinia odnosi się do stanu prawnego z dnia jej wystawienia.
4. Opinia dotyczy wyłącznie przepisów prawa Unii Europejskiej.
5. Jakkolwiek wnioski zaprezentowane w Opinii wynikają z analizy przepisów oraz wypowiedzi prezentowanych w doktrynie prawniczej, a także tez orzeczeń sądowych, jednakże sąd wydający orzeczenie w konkretnej sprawie nie musi uwzględniać poglądów wyrażonych przez autora Opinii, przez organy władzy publicznej sformułowane w związku z wydawaniem orzeczenia w innej sprawie ani stanowiska prezentowanego w literaturze prawniczej.

[21] Wyrok z dnia 30 kwietnia 1996 r. w sprawie C-194/94, *CIA Security International*, pkt 47. Co istotne, pomimo obowiązku notyfikowania całego projektu aktu prawnego, sankcja bezskuteczności rozciąga się wyłącznie na przepisy techniczne, a nie cały już przyjęty akt prawny.