Ekspertyza dotycząca analizy przepisów dyrektywy NIS 2 w porównaniu do projektu przedstawionego przez Ministerstwo Cyfryzacji – różnice i wnioski

Autor: dr hab. Marcin Górski, prof. UŁ, radca prawny

Łódź, 3 września 2024 r.

Ekspertyzę sporządzono na zlecenie Stowarzyszenia Obywatelskiego „Dom Polski" („**Klient**"). Stanowiska prezentowane w ekspertyzie odzwierciedlają wyłącznie poglądy jej autora dotyczące interpretacji prawa i nie muszą być reprezentatywne dla podmiotów, w których autor jest zatrudniony albo z którymi współpracuje.

Znaczenie wyrażeń użytych w ekspertyzie

Następujące wyrażenia użyte w ekspertyzie mają następujące znaczenie, o ile wyraźnie nie zaznaczono odmiennie:

1) **Ustawa** – ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t. j. w Dz. U. z 2024 r. poz. 1077;
2) **Projekt** – projekt z 23 kwietnia 2024 r. ustawy o zmianie ustawy o krajowym systemie cybezbezpieczeństwa oraz niektórych innych ustaw (https://legislacja.rcl.gov.pl/projekt/12384504/katalog/13055207#13055207, wyświetlono 29 sierpnia 2024 r.);
3) **Dyrektywa** – dyrektywa PE i Rady (UE) 2022/2055 z 14 grudnia 2014 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) (Tekst mający znaczenie dla EOG) (Dz. Urz. UE z 27 grudnia 2022 r., L 333 s. 80);

1. Przedmiot ekspertyzy

Przedmiotem ekspertyzy, zgodnie z oczekiwaniami Klienta, jest przedstawienie generalnych uwag dotyczących Dyrektywy, jej podstaw, celów i kluczowych rozwiązań dotyczących sytuacji jednostek, a także wyjaśnienie, w jakim zakresie ujawniają się różnice pomiędzy Projektem, którego celem jest transponowanie Dyrektywy do Ustawy, a Dyrektywą, jak również zakreślenie możliwych konsekwencji tych różnic.

2. Uwagi wstępne

Opinia nie podejmuje zagadnienia oceny zgodności projektowanych przepisów z Konstytucją RP, czy też spójności regulacyjnej w perspektywie systemowej. Opinia nie odnosi się również do oceny zgodności Projektu z innymi aktami prawa UE niż sama Dyrektywa. Nie dotyczy ona również badania zgodności Projektu z Konwencją o cyberprzestępczości[1]. Opinia dotyczy wyłącznie oceny zgodności projektu z Dyrektywą, przy czym sygnalizuje możliwe niezgodności z prawem pierwotnym UE, a to z uwagi na wyrażony w motywie 143 Dyrektywy obowiązek jej wdrażania zgodnie z normami prawa pierwotnego Unii. Należy też dodać, że termin przygotowania ekspertyzy był bardzo krótki, co może sposób nieunikniony wpływać na jakość jej wniosków, a co wynika z pewnego pośpiechu w prowadzeniu prac legislacyjnych. Projekt został wszak opublikowany dopiero 24 kwietnia 2024 r., podczas gdy skutki przyjęcia projektowanych zmian legislacyjnych dla różnych sektorów gospodarki są intensywne, a termin transpozycji Dyrektywy upływa 17 października 2024 r. (z obowiązkiem stosowania nowych przepisów już od 18 października 2024 r., co – z uwagi na zasadę pewności prawa – powinno wymusić ich uchwalenie najpóźniej do końca września 2024 r.).

[1] Konwencja o cybeprzestępczości, sporządzona w Budapeszcie 23 listopada 2001 r., Dz. U. z 2015 r. poz. 728. Konwencja ta, zawarta w systemie Rady Europy, zobowiązuje do penalizacji określonych typów cyberprzestępstw, a także reguluje współpracę międzynarodową w tym obszarze.

Te krytyczne uwagi nie dotyczą powolności obecnego rządu w procedowaniu Projektu, lecz raczej tego, że trud transpozycji Dyrektywy z grudnia 2024 r. musiał zostać podjęty w ostatnim półroczu przed obowiązującym terminem transpozycji, co należy ocenić jako silnie niepokojące, chociaż zarazem niejako „standardowe". Nie wzbudzałoby to może aż tak silnych zastrzeżeń, gdyby nie wspomnianej wyżej skutki gospodarcze.

Ekspertyzę podzielono na części dotyczące wyjaśnienia celu i sposobu harmonizacji przyjętego w Dyrektywie (cz. 3.1. Ekspertyzy), jej zakładanego zakresu podmiotowego, rozumianego jako określenie kręgu podmiotów, których mają dotyczyć obowiązki wprowadzane krajowymi regulacjami transpozycyjnymi (cz. 3.2. Ekspertyzy), kluczowych rozwiązań regulacyjnych zawartych w Ekspertyzie (cz. 3.3. Ekspertyzy) oraz wskazania niektórych wątpliwości, co do zgodności Projektu z Dyrektywą (cz. 4 Ekspertyzy). Ostatnim fragmentem (cz. 5 Ekspertyzy) są krótkie wnioski dotyczące rekomendacji odnośnie do dalszego procedowania Projektu w Radzie Ministrów i w toku prac parlamentarnych.

3. Kluczowe parametry Dyrektywy

3.1. Cel i sposób harmonizacji

Zasadniczym celem Dyrektywy jest osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, aby poprawić funkcjonowanie rynku wewnętrznego[2]. Realizując ten cel, Dyrektywa zastępuje dotychczasową dyrektywę 2016/1148[3], którą oceniono jako niewystarczającą z uwagi na możliwe rozbieżności, bo z jej przeglądu wynikało, że

> „istnieją znaczne rozbieżności w jej wdrażaniu przez państwa członkowskie, w tym pod względem jej zakresu, którego ustalenie w znacznej mierze pozostawiono do uznania państw członkowskich. W dyrektywie (UE) 2016/1148 zapewniono państwom członkowskim bardzo duży margines swobody także w odniesieniu do wdrażania ustanowionych w niej obowiązków dotyczących bezpieczeństwa i zgłaszania incydentów. W rezultacie obowiązki te zostały wdrożone na poziomie krajowym w bardzo różny sposób. Podobne rozbieżności we wdrażaniu wystąpiły w odniesieniu do przepisów dyrektywy (UE) 2016/1148 dotyczących nadzoru i egzekwowania prawa. Wszystkie te rozbieżności pociągają za sobą fragmentację rynku wewnętrznego i mogą szkodliwie wpływać na jego funkcjonowanie, oddziałując w szczególności na transgraniczne świadczenie usług i poziom cyberodporności ze względu na stosowanie zróżnicowanych środków. Ostatecznie rozbieżności te mogą prowadzić do większej podatności niektórych państw członkowskich na cyberzagrożenia, co może wywołać reperkusje dla całej Unii”[4].

[2] Zob. art. 1 ust. 1 Dyrektywy.

[3] Dyrektywa PE i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE z 19 lipca 2016 r., L 194, s. 1.

[4] Zob. motywy 4 i 5 Dyrektywy.

Jednocześnie w art. 5 Dyrektywy wskazano, że jest ona środkiem tzw. harmonizacji minimalnej[5], a zatem „nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne (ang. *are consistent*, franc. *soient compatibles*) z obowiązkami państw członkowskich, ustanowionymi w prawie Unii". Oznacza to, że dopuszczalne jest wprowadzenie albo utrzymanie przez państwa członkowskie UE regulacji zgodnych z prawem UE (w tym prawem pierwotnym), których rezultatem jest zapewnienie wyższego poziomu cyberbezpieczeństwa, niż wynikający z Dyrektywy. Samo pojęcie cyberbezpieczeństwa oznacza zaś, zgodnie z art. 6 pkt 3 Dyrektywy w zw. z art. 2 pkt 1 rozporządzenia 2019/881[6], „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami". Skoro więc Dyrektywa dopuszcza wprowadzanie środków krajowych skutkujących wyższym poziomem cyberbezpieczeństwa, zaś samo cyberbezpieczeństwo to „działania", o których mowa w powołanym przepisie rozporządzenia 2019/881, to nie jest jednoznaczna odpowiedź na pytanie o to, czy dopuszczalne jest rozszerzenie zakresu podmiotowego określonego w art. 2 Dyrektywy.

Z jednej strony, wprowadzenie standardu minimalnego nie wyklucza rozszerzenia zakresu środka transpozycyjnego poza zakres *ratione materiae* wymagany środkiem transponowanym, przy czym należałoby traktować taki przypadek jako tzw. *gold plating* i uznać, że mamy wówczas do czynienia z realizacją krajowej swobody implementacyjnej[7].

Z drugiej jednak strony omawiana tu Dyrektywa jest motywowana celem eliminacji różnic, które uznano za niepożądane nie tylko ze względu na nieodpowiednie poziomy cyberbezpieczeństwa w poszczególnych państwach członkowskich, ale również z uwagi na zakłócenia w funkcjonowaniu rynku wewnętrznego (zob. cytowany wyżej fragment motywów Dyrektywy: „te rozbieżności pociągają za sobą fragmentację rynku wewnętrznego i mogą szkodliwie wpływać na jego funkcjonowanie, oddziałując w szczególności na transgraniczne świadczenie usług"). Ponadto, za stanowiskiem negującym rozszerzanie

[5] Zob. szerzej F. de Cecco, *Room to Move? Minimum harminisation and fundamental rights,* CMLRev. 2006, nr 43, s. 9-30.

[6] Rozporządzenie PE i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Tekst mający znaczenie dla EOG) (Dz. Urz. UE z 7 czerwca 2019 r., L 151, s. 15.

[7] Por. wyrok TS z 14 marca 1991 r., C-361/89 *Di Pinto,* pkt 19 i 21-23.

zakresu podmiotowego środków transpozycyjnych przemawiają motywy 7[8] i 17[9] Dyrektywy, które precyzują sposób interpretacji art. 2 Dyrektywy w relacji do jej art. 5, a także art. 2 ust. 2 lit. b) – e) w zw. z art. 3 ust. 1 lit. e) Dyrektywy. Wreszcie, za takim ujęciem przemawia także wykładnia historyczna, porównująca obecny art. 2 Dyrektywy do art. 5 dyrektywy 2016/1148.

Należy zatem zasygnalizować już w tym miejscu wątpliwość dotyczącą dopuszczalności, w tym akurat przypadku, ekstensji zakresów podmiotowych krajowych przepisów harmonizacyjnych ponad zakres wyznaczony przepisem art. 2 Dyrektywy.

3.2. Zakres podmiotowy

Zdekodowanie zakresu podmiotowego Dyrektywy wymaga łącznego odczytania art. 2 w zw. z art. 3 Dyrektywy i w zw. z załącznikami I i II Dyrektywy, przy czym może on ulegać rozszerzeniu na mocy art. 2 ust. 3 Dyrektywy w przypadku zdefiniowania przez państwo członkowskie podmiotów krytycznych w wykonaniu art. 6 dyrektywy 2022/2057[10] – wówczas Dyrektywę stosuje się także i do tych podmiotów.

Podstawowym elementem tego zakresu są podmioty kluczowe i ważne, zdefiniowane w art. 3 Dyrektywy, będące co najmniej średnimi przedsiębiorstwami w rozumieniu art. 2 załącznika do zalecenia 2003/361/WE[11] i świadczące usługi lub prowadzące działalność w UE.

[8] Zgodnie z tym motywem, „Na podstawie dyrektywy (UE) 2016/1148 państwa członkowskie były odpowiedzialne za identyfikację podmiotów spełniających kryteria pozwalające na uznanie ich za operatorów usług kluczowych. Aby wyeliminować znaczne rozbieżności pod tym względem między państwami członkowskimi oraz zapewnić wszystkim podmiotom objętym regulacją pewność prawa w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie i do obowiązków dotyczących zgłaszania incydentów, należy ustanowić jednolite kryterium określające, które podmioty są objęte zakresem stosowania niniejszej dyrektywy".

[9] Zgodnie z tym motywem „Państwa członkowskie powinny mieć możliwość decydowania, że za podmioty kluczowe należy uznać podmioty zidentyfikowane przed wejściem w życie niniejszej dyrektywy jako operatorzy usług kluczowych zgodnie z dyrektywą (UE) 2016/1148".

[10] Dyrektywa PE i Rady (UE) 2022/2057 z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Tekst mający znaczenie dla EOG) (Dz. Urz. UE z 27 grudnia 2022 r., L 333, s. 164).

[11] Zalecenie KE 2003/361/EC z 6 maja 2003 r. w sprawie definicji mikro-, małych i średnich przedsiębiorstw, Dz. Urz. UE z 20 maja 2003 r., L 124, s. 36.

Przedsiębiorstwa te kwalifikuje się jako kluczowe albo ważne, zgodnie z art. 3 ust. 1 i 2 Dyrektywy. Oprócz nich, Dyrektywa stosuje się również do:

a) podmiotów „w rodzaju tych, o których mowa w załączniku I lub II" (a więc takich, które, które prowadzą działalność w sektorach kluczowych albo ważnych, zgodnie z tymi załącznikami), spełniających albo nie warunki dotyczące wielkości, ale jednocześnie spełniających co najmniej jedno z kryteriów kwalifikacyjnych z art. 2 ust. 2 Dyrektywy; oraz
b) podmiotów zdefiniowanych jako krytyczne na mocy Dyrektywy 2022/2557; oraz
c) podmiotów świadczących usługi rejestracji nazw domen, niezależnie od ich wielkości.

Wreszcie, zgodnie z art. 2 ust. 3 Dyrektywy, państwa członkowskie mogą rozszerzyć zakres podmiotowy stosowania Dyrektywy na podmioty administracji publicznej na poziomie lokalnym oraz instytucje edukacyjne. Natomiast art. 2 ust. 9 i 10 Dyrektywy określają wyłączenia z zakresu podmiotowego.

3.3. Kluczowe rozwiązania regulacyjne

Dyrektywa, poza wyeliminowaniem swobody regulacyjnej państw członkowskich w identyfikowaniu „operatorów usług kluczowych"[12], definiuje podstawowe dla dziedziny pojęcia (tych definicji jest ponad dwukrotnie więcej, niż w dyrektywie 2016/1148), doprecyzowuje obowiązki państw w zakresie zarządzania cyberbezpieczeństwem, doprecyzowuje obowiązki dotyczące funkcjonowania tzw. zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT[13]), rozbudowuje znacząco regulację odnoszącą się do współpracy na poziomie unijnym i międzynarodowym, jak również wprowadza szczegółową i ekstensywną regulację dotyczącą środków zarządzania ryzykiem w cyberbezpieczeństwie, obejmującą szereg obowiązków, które państwa członkowskie muszą nałożyć na podmioty kluczowe i ważne. W sposób znany już z obszaru danych osobowych, Dyrektywa określa warunki nakładania sankcji administracyjnych oraz wymagania odnoszące

[12] Zob. art. 5 dyrektywy 2016/1148.
[13] Skrót pochodzący od „Computer Security Incident Response Teams".

się do środków penalnych. Dyrektywa modyfikuje również, na tle dotychczasowego stanu prawnego, sposób określenia jurysdykcji państwa członkowskiego wobec danego podmiotu, uzależniając ją od „miejsca prowadzenia działalności”[14], które rozumie się jako państwo członkowskie (zob. art. 26 ust. 2 Dyrektywy, kursywę dodano):

> „w którym *przeważnie podejmuje decyzje związane ze środkami zarządzania ryzykiem w cyberbezpieczeństwie*. Jeżeli nie można ustalić takiego państwa członkowskiego lub jeżeli takich decyzji nie podejmuje się w Unii, uznaje się, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym *prowadzone są działania w zakresie cyberbezpieczeństwa*. Jeżeli nie można ustalić takiego państwa członkowskiego, uznaje się, że główne miejsce prowadzenia działalności znajduje się w państwie członkowskim, w którym *dany podmiot ma miejsce prowadzenia działalności o największej liczbie pracowników w Unii*”.

Jeśli zaś dany podmiot nie ma miejsca prowadzenia działalności w UE, to (art. 26 ust. 3 Dyrektywy) musi wyznaczyć przedstawiciela w UE i jurysdykcja państwa członkowskiego jest wyznaczana według kryterium miejsca prowadzenia działalności przez niego (co, jak się wydaje, ustala się z kolei w oparciu o kryteria w art. 26 ust. 2 Dyrektywy), a jeżeli nie został on wyznaczony, wówczas jurysdykcję sprawuje każde państwo, w którym podmiot świadczy usługi.

[14] Zob. art. 26 Dyrektywy.

4. Analiza Projektu na tle Dyrektywy

Projekt, jak już wspomniano, ma na celu zmianę m.in. Ustawy w celu wdrożenia Dyrektywy. Jednak Projekt wykracza poza ten cel, w związku z czym załączono do niego odwróconą tabelę zgodności[15]. W toku prac nad Projektem zgłoszono jego krytykę koncentrującą się na zarzutach rozszerzenia obowiązków, których nałożenie na przedsiębiorców zakładała Dyrektywa, o obowiązki w niej nie przewidziane[16].

Analizując projekt nieco bardziej szczegółowo, należy zwrócić uwagę, w szczególności, na następujące różnice pomiędzy regulacją Dyrektywy i Projektem:

1) W art. 1 pkt 2 lit. a) Projektu zawarto definicję „bezpieczeństwa systemów informacyjnych" (nowy art. 2 pkt 3c Ustawy), w następującym brzmieniu: „odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy"; tymczasem art. 6 pkt 2) Dyrektywy wskazuje, że bezpieczeństwo, o którym w nim mowa, ma dotyczyć nie tylko usług oferowanych przez same systemy, ale również usług „dostępnych za ich pośrednictwem";
2) W art. 1 pkt 2 lit. e) Projektu zawarto definicję *incydentu w cyberbezpieczeństwie na dużą skalę* (nowy art. 2 pkt 8 Ustawy), która rozszerza zakres przedmiotowy definiendum poza granice wymagane Dyrektywą – zgodnie z art. 6 pkt 7 Dyrektywy przekroczenie zdolności reagowania państwa nie jest abstrakcyjne, lecz ma dotyczyć

[15] W przypadku gold platingu transpozycyjnego ma zastosowanie § 30 ust. 2 Regulaminu Pracy Rady Ministrów (M. P. z 2022 r. poz. 348), zgodnie z którym „Projekt ustawy mającej na celu wdrożenie lub służącej stosowaniu prawa Unii Europejskiej może zawierać przepisy wykraczające poza ten cel wyłącznie w szczególnie uzasadnionych przypadkach. W takim przypadku organ wnioskujący dołącza do projektu dodatkowo tabelaryczne zestawienie projektowanych przepisów ustawy, które wykraczają poza cel wdrożenia lub zapewnienia stosowania prawa Unii Europejskiej, wraz z wyjaśnieniem niezbędności objęcia ich tym projektem, zwane dalej "odwróconą tabelą zgodności".".

[16] Zob. P. Szymaniak, *Nowa ustawa rządu w ogniu krytyki. Wymusi na firmach milionowe wydatki*, Rzeczpospolita, 3 lipca 2024 r., źródło https://www.rp.pl/abc-firmy/art40755541-nowa-ustawa-rzadu-w-ogniu-krytyki-wymusi-na-firmach-milionowe-wydatki, dostęp 3 września 2024 r.

samego incydentu, zaś wpływ na państwa członkowskie ma dotyczyć co najmniej 2 państw członkowskich, tymczasem definicja zawarta w Projekcie dopuszcza wpływ tylko na inne państwo członkowskie, bez wpływu na cyberbezpieczeństwo w samej Rzeczypospolitej Polskiej;

3) W art. 1 pkt 2 lit h) Projektu nie jest jasne, dlaczego odesłanie ograniczono wyłącznie do przepisów ustawy – Prawo o szkolnictwie wyższym i nauce, a już nie do art. 2 ustawy z 30 kwietnia 2010 r. o instytutach badawczych (t.j. w Dz. U. z 2024 r. poz. 534), chociaż trzeba zauważyć, że z punktu widzenia Dyrektywy taki wybór mieści się w granicach swobody implementacyjnej wynikających z art. 2 ust. 5 lit. b) Dyrektywy;
4) W art. 1 pkt 5 Projektu (dotyczącym dodania nowego art. 3a w brzmieniu „W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usług") wyrażono założenie, znajdujące zasadniczo oparcie zwłaszcza w treści art. 6 pkt 8) Dyrektywy, zgodnie z którym podmioty krajowego systemu cyberbezpieczeństwa będą upoważnione do podejmowania działań „w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu"; wątpliwości dotyczą gwarancji ochrony prywatności w tym kontekście, w szczególności rzeczywistej dostępności środków ochrony prawnej dla zainteresowanych jednostek, co jest wymagane dla zgodności przewidzianej Projektem ingerencji w szczególności z art. 47 Karty Praw Podstawowych UE;
5) W art. 1 pkt 8 Projektu zawarto projektowane zastąpienie dotychczasowej treści art. 5 Ustawy nową treścią, która ma odpowiadać art. 3 Dyrektywy; na wstępie należy podzielić zastrzeżenia wyrażone przez RCL w toku opiniowania Projektu, zgodnie z którymi „niezrozumiałe jest dlaczego zarówno podmiot kluczowy jak i podmiot ważny jest definiowany przez jednoczesne odesłanie do obu załączników. Zgodnie ze wskazanymi załącznikami do ustawy, określają one podmioty kluczowe (załącznik nr 1) i podmioty ważne (załącznik nr 2). Zwrócić należy też uwagę, że zgodnie z projektowanym art. 7c ust. 2 - podmiot uznaje się za podmiot kluczowy, jeżeli prowadzi działalność określoną w załączniku nr 1 do ustawy, a za podmiot ważny -

jeżeli prowadzi działalność określoną w załączniku nr 2 do ustawy”[17]. Ponadto należy zauważyć, że katalog podmiotów kluczowych zawarty w załączniku nr 1 do projektu jest szerszy, niż jego odpowiednik w załączniku I do Dyrektywy, obejmując dodatkowo przedsiębiorców działających w następujących sektorach: Produkcja, wytwarzanie i dystrybucja chemikaliów, Produkcja, przetwarzanie i dystrybucja żywności, produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, produkcja komputerów, wyrobów elektronicznych i optycznych, produkcja urządzeń elektrycznych, produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana, produkcja pojazdów samochodowych, przyczep i naczep, produkcja pozostałego sprzętu transportowego; biorąc pod uwagę zastrzeżenia zawarte w pkt 3.1. niniejszej ekspertyzy, to rozszerzenie podmiotowe wzbudza wątpliwości z punktu widzenia celu Dyrektywy;

6) W art. 1 pkt 11 Projektu zawarto projektowaną treść nowego art. 7c Ustawy, zgodnie z którą możliwe będzie dokonanie z urzędu, decyzją organu właściwego ds. cyberbezpieczeństwa, uznanie podmiotu za kluczowy lub ważny, przy czym decyzja ta ma być zaopatrzona w rygor natychmiastowej wykonalności ex lege, co będzie skutkować obowiązkiem realizacji obowiązków ustawowych w terminie 6 miesięcy i zapewnienia przeprowadzenia na koszt takiego podmiotu audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług (projektowany art. 15 Ustawy w brzmieniu nadanym zgodnie z art. 1 pkt 20 Projektu); odnosząc się do tej części Projektu należy podzielić uwagi zgłoszone przez Rzecznika Praw Obywatelskich[18], nadto zaś zauważyć, że w braku ustawowego określenia choćby instrukcyjnego terminu dla rozpatrzenia skargi w drodze postępowania sądowoadministracyjnego, ochrona prawna udzielona prawu własności zainteresowanych podmiotów oraz ich swobodzie działalności gospodarczej jawi się jako iluzoryczna;
7) W art. 1 pkt 13 Projektu przewidziano delegację ustawową dla Rady Ministrów do określenia „w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub podmioty ważne szczegółowe wymagania

[17] Zob. dokument w https://legislacja.rcl.gov.pl/docs//2/12384504/13055195/13055198/dokument670632.pdf, s. 2, dostęp 3 września 2024 r.

[18] Zob. https://legislacja.rcl.gov.pl/docs//2/12384504/13055207/13055210/dokument675899.pdf, dostęp 3 września 2024 r.

dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA", skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo" – przy czym „wzięcie pod uwagę" to dużo mniej niż „zgodność" czy choćby „uwzględnienie", a to skutkuje wątpliwościami dotyczącymi nadmiernej swobody egzekutywy w konstruowaniu normatywnej ingerencji w zakres wolności gospodarczej zainteresowanych podmiotów;

8) W art. 1 pkt 13 Projektu zawarto również regulację projektowanego art. 8b ust. 3, zakładającą obiektywną odpowiedzialność kierownika podmiotu[19] kluczowego lub ważnego za wykonywanie obowiązków w zakresie cyberbezpieczeństwa wynikających z przepisów wskazanych w projektowanym ustępie 1 tego artykułu Ustawy; taka konstrukcja wzbudza wątpliwości z punktu widzenia zasady skuteczności (efektywnej sankcji), którą zabezpiecza art. 34 ust. 1 Dyrektywy. Ponadto, wątpliwości wzbudza także projektowany art. 8d i art. 8e Ustawy (zmiana wynikająca z art. 1 pkt 13 Projektu), ponieważ przesądza o dystrybucji zadań w obrębie podmiotu kluczowego lub ważnego, czego nie wymaga art. 20 Dyrektywy – ten ostatni przepis wskazuje bowiem tylko, że „państwa członkowskie zapewniają, aby organy zarządzające podmiotów kluczowych i ważnych zatwierdzały środki zarządzania ryzykiem w cyberbezpieczeństwie przyjęte przez te podmioty w celu zapewnienia zgodności z art. 21, nadzorowały ich wdrażanie i mogły być pociągnięte

[19] Projektowany art. 2 pkt 8a Ustawy odsyła w zakresie definicji tego pojęcia do art. 3 pkt 6 ustawy o rachunkowości (w istocie chodzi zpewne o art. 3 ust. 1 pkt 6 tej ustawy), zgodnie z którym „rozumie się przez to członka zarządu lub innego organu zarządzającego, a jeżeli organ jest wieloosobowy – członków tego organu, z wyłączeniem pełnomocników ustanowionych przez jednostkę. W przypadku spółki jawnej i spółki cywilnej za kierownika jednostki uważa się wspólników prowadzących sprawy spółki, w przypadku spółki partnerskiej – wspólników prowadzących sprawy spółki albo zarząd, a w odniesieniu do spółki komandytowej i spółki komandytowo-akcyjnej – komplementariuszy prowadzących sprawy spółki. W przypadku osoby fizycznej prowadzącej działalność gospodarczą za kierownika jednostki uważa się tę osobę; do osób wykonujących wolne zawody przepis ten stosuje się odpowiednio. Za kierownika jednostki uważa się również likwidatora, a także syndyka lub zarządcę ustanowionego w postępowaniu restrukturyzacyjnym oraz zarządcę sukcesyjnego, o którym mowa w ustawie z dnia 5 lipca 2018 r. o zarządzie sukcesyjnym przedsiębiorstwem osoby fizycznej i innych ułatwieniach związanych z sukcesją przedsiębiorstw, albo osobę, o której mowa w art. 14 tej ustawy, która dokonała zgłoszenia, o którym mowa w art. 12 ust. 1c ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. z 2022 r. poz. 166, 1301 i 1933)".

do odpowiedzialności za naruszanie przez te podmioty tego artykułu" (ust. 1), oraz że „państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom", co nie jest równoznaczne ani np. z nałożeniem na kierowników podmiotów obowiązku „podejmowania decyzji", o których mowa w projektowanym art. 8d pkt 1, ani też z odpowiedzialnością osobistą każdego z członków organu zarządzającego podmiotu, niezależnie od przyjętego w takim organie podziału zadań i odpowiedzialności;

9) W art. 1 pkt 43 Projektu zawarto zmianę brzmienia art. 43 ust. 1 Ustawy, którą należy odczytywać łącznie z projektowanym art. 53c ust. 2 i 3 Ustawy (dodane przez art. 1 pkt 57 Projektu), a która będzie skutkować skróceniem terminu udzielenia informacji do wstępnej oceny, czy podmiot należy kwalifikować jako kluczowy albo ważny, do minimum 7 dni (w miejsce obecnych 14 dni – zob. art. 43 ust. 3 Ustawy w brzmieniu obowiązującym); tak krótki termin nie jest wymagany Dyrektywą, a zarazem wzbudza wątpliwości z punktu widzenia zasady proporcjonalności ingerencji w wolność działalności gospodarczej (art. 16 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE);
10) Takie same wątpliwości (tj. co do proporcjonalności ingerencji w swobodę chronioną przez art. 16 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE) wzbudza art. 1 pkt 46 Projektu w zakresie dotyczącym projektowanego brzmienia art. 46 ust. 6 Ustawy, zgodnie z którym dostosowanie się przez podmioty kluczowe i ważne do wymagań technicznych i funkcjonalnych korzystania z systemu teleinformatycznego wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa ma nastąpić w terminie 3 miesięcy od udostępnienia wymagań tego systemu przez ministra właściwego ds. informatyzacji;
11) Również podobne wątpliwości wzbudza art. 1 pkt 56 Projektu w zakresie projektowanego brzmienia art. 53 ust. 5 pkt 5 Ustawy, w którym zrezygnowano – w porównaniu z art. 33 ust. 4 lit. f) Dyrektywy – z doprecyzowania, że termin wdrożenia zaleceń audytowych, określony decyzją, ma być „rozsądny"; jednocześnie należy

zauważyć, że dookreślenie w projektowanej treści przepisu Ustawy, że każdy z terminów realizacji obowiązków, o których mowa w projektowanym art. 53 ust. 5, powinien być „rozsądny", jest obowiązkiem wynikającym z zasady ogólnej prawa UE, jaką jest zasada proporcjonalności, o czym przypominają motywy 81, 82 i 127 Dyrektywy, przy czym należy uznać, że zawarta w art. 1 pkt 56 Projektu regulacja wzbudza wątpliwości co do spełnienia tych wymogów, zaś treść zawarta w projektowanym art. 53 ust. 10 Ustawy tych wątpliwości całkowicie nie usuwa, bo zawarte tam „parametry" nie odnoszą się w sposób wyraźny również do określenia terminów wykonania zobowiązań, o których mowa w projektowanym art. 53 ust. 5 Ustawy;

12) Art. 1 pkt 56 Projektu wzbudza również wątpliwości w zakresie projektowanego brzmienia art. 53 ust. 8 pkt 4 Ustawy (orzeczenie zakazu zajmowania stanowiska), bo nie jest jasne, który sąd i w jakim trybie miałby orzekać „tymczasowy zakaz zajmowania stanowiska", jakie to miałoby być stanowisko, ani też, czy orzeczenie to miałoby status postanowienia zabezpieczającego (a więc wydawanego bez udziału zainteresowanej osoby *ex ante*), czy też merytorycznego, nie wspominając już o tym, że nie wiadomo też, jaki miałby być zakres czasowy tej „tymczasowości"; wszystko to składa się na wątpliwość co do zgodności projektowanej regulacji z art. 47 Karty Praw Podstawowych UE (zob. motyw 143 Dyrektywy); wątpliwości te potęguje projektowany art. 53 ust. 11 w zw. z ust. 13 Ustawy (możliwość odstąpienia od poinformowania o wstępnych ustaleniach, a zarazem ograniczenie obowiązku – co do zasady – informowania do samych podmiotów kluczowych, podczas gdy środek przewidziany w projektowanym art. 53 ust. 8 pkt 4 Ustawy jest adresowany do osób kierujących podmiotem kluczowym, co zresztą jest pojęciem dużo szerszym niż „kierownik podmiotu", o którym mowa w);

13) Art. 1 pkt 58 Projektu w zakresie, w jakim określa on maksymalny czas kontroli w roku kalendarzowym jako 48 dni roboczych[20], wzbudza wątpliwości na kilku poziomach: po pierwsze, skoro reagowanie na cyberzagrożenia powinno być szybkie[21], to zupełnie niezrozumiała jest dopuszczona w Projekcie „ślamazarność"

[20] Ten czas maksymalny przewidziano wobec przedsiębiorców większych niż średni, zgodnie z art. 55 ust. 1 pkt 4 ustawy z 6 marca 2018 r. – Prawo przedsiębiorców, t. j. w Dz. U. z 2024 r. poz. 236.

[21] Zob. motywy 58 i 70 Dyrektywy.

kontroli; po drugie, skoro Dyrektywa zakłada nałożenie obowiązków również na średnie przedsiębiorstwa w rozumieniu prawa UE, to niezrozumiałe jest określenie terminu kontroli właściwego według ogólnych reguł prawa polskiego w przypadku przedsiębiorców większych niż średni; po trzecie, skoro Dyrektywa zakłada minimalizację uciążliwości kontroli[22], to niezrozumienie wzbudza zakreślenie terminu kontroli w maksymalnym zakresie przewidzianym prawem krajowym;

14) Art. 1 pkt 59 Projektu, zakładający nałożenie na kontrolowany podmiot ciężaru finansowego tłumaczeń dokumentacji, wzbudza wątpliwość co do proporcjonalności ingerencji w prawo własności (art. 17 ust. 1 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE), przy czym inaczej niż w przypadku kosztów ukierunkowanego audytu Dyrektywa nie przewiduje w tym przypadku przerzucenia kosztów na podmiot kontrolowany[23], zaś biorąc pod uwagę założoną w Dyrektywie spójność ciężarów nakładanych na podmioty kluczowe i ważne w skali UE[24] może to z kolei czynić wątpliwym osiągnięcie jednego z zasadniczych celów Dyrektywy;
15) Art. 1 pkt 60 Projektu, w zakresie dotyczącym projektowanego brzmienia art. 58 ust. 4 Ustawy, wzbudza *a limine* wątpliwości z punktu widzenia zasady proporcjonalności, bo trudno wytłumaczyć, dlaczego w jednym akcie zakłada się prowadzenie czynności kontrolnych przez maksymalnie 48 dni roboczych, z jednoczesnym ograniczeniem możliwości składania zastrzeżeń do ustaleń takiej kontroli do 7 dni kalendarzowych (czyli, niekiedy, np. 3 dni roboczych, przy nagromadzeniu w danym tygodniu kilku dni ustawowo wolnych od pracy); nie sposób postulować w takich okolicznościach zachowanie „równości broni", bo oczywiście nie jest to relacja *inter partes*, lecz porównanie normatywnego określenia sytuacji prawnej jednostki na tle sytuacji prawnej organu, ale takie zróżnicowanie sytuacji kontrolującego i kontrolowanego może wzbudzać zastrzeżenia co do efektywnej dostępności środka ochrony prawnej;

[22] Zgodnie z motywem 123 Dyrektywy, „Wykonywanie zadań nadzorczych przez właściwe organy nie powinno niepotrzebnie utrudniać działalności prowadzonej przez dany podmiot. W przypadku gdy właściwe organy wykonują zadania nadzorcze w odniesieniu do podmiotów niezbędnych, w tym prowadzenie kontroli na miejscu i nadzoru zdalnego, badanie naruszeń niniejszej dyrektywy, przeprowadzanie audytów bezpieczeństwa lub skanowanie bezpieczeństwa, powinny one minimalizować wpływ tych czynności na działalność gospodarczą danego podmiotu".

[23] Zob. art. 32 ust. 2, zdanie końcowe, oraz art. 33 ust. 2, zdanie końcowe, Dyrektywy.

[24] Zob. rozdz. 3.1. ekspertyzy.

wątpliwości te potęguje utrzymanie niedostępności środka zaskarżenia wobec zaleceń pokontrolnych[25];

16) Najwięcej zastrzeżeń i największym ciężarze gatunkowym wzbudza art. 1 pkt 70 Projektu, wprowadzający nowe art. 67a – 67k Ustawy, dotyczące szczególnych działań na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym; regulacja ta nie stanowi transpozycji Dyrektywy[26]; w tym zakresie należy zwrócić szczególną uwagę na:
    a) Projektowany art. 67a ust. 1 Ustawy, który będzie pozwalał na określenie zakresu podmiotowego rekomendacji do „kategorii podmiotów", przy czym samo pojęcie „kategorii" nie zostało w ustawie zdefiniowane, co może pozwolić na celowanie nakładanych obowiązków na określonych przedsiębiorców albo ich grupy, zależnie od potrzeb politycznych; ponadto, przepis ten nie nakłada na pełnomocnika obowiązku zachowania wymogów proporcjonalności, co może skutkować nałożeniem obowiązków nadmiernych w danych okolicznościach i stanowić nadmierną ingerencję w wolności gospodarcze chronione przez art. 16 i 17 Karty Praw Podstawowych UE (co z kolei może naruszać art. 52 ust. 1 Karty);
    b) Projektowany art. 67a ust. 4 Ustawy, który zakłada związanie adresata rekomendacjami, bez jakiejkolwiek przewidzianej ustawą drogi sądowej do ich zaskarżenia, co wzbudza wątpliwości co do zgodności z art. 47 Karty Praw Podstawowych UE;
    c) Projektowany art. 67b Ustawy, dotyczący uznania dostawców sprzętu lub oprogramowania za dostawców wysokiego ryzyka; projektowane przepisy wzbudzą wątpliwości m.in. co do zgodności z art. 41 Karty Praw Podstawowych UE (zasada dobrej administracji), w zakresie, w jakim organy krajowe powinny

[25] Art. 59 ust. 2 Ustawy.

[26] Jak wskazano w odwróconej tabeli zgodności (s. 32), „Przepisy te dodają możliwość wydawania przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Wprowadza się instytucję postępowania w sprawie uznania za dostawcę wysokiego ryzyka, co stanowi wdrożenie unijnego Toolboxa 5g. Reguluje się także kwestie dotyczące monitorowania przez organy właściwe do spraw cyberbezpieczeństwa wykonania polecenia zabezpieczającego. Wprowadza się także możliwość przekazania niektórych zadań CSIRT poziomu krajowego do Ministra Obrony Narodowej".

uwzględniać standard zasady ogólnej[27] prawa do dobrej administracji wykonując prawo UE[28] (abstrahując w tym miejscu od sporu o zakres związania organów krajowych tą *zasadą*, a także wątpliwości dotyczących zakresu jej zastosowania do przepisów stanowiących transpozycyjny *gold plating*, jak w tym przypadku), podczas gdy projektowany przepis zakłada m.in. fikcję prawną zawiadomienia o wszczęciu postępowania w przypadku podmiotów spoza UE/Szwajcarii/EFTA-EOG (projektowany art. 67b ust. 8 Ustawy), brak obowiązku powiadomienia strony o miejscu i terminie przeprowadzenia dowodu ze świadków, biegłych lub oględzin przynajmniej na siedem dni przed terminem, a także brak obowiązku umożliwienia jej korzystania z uprawnień wynikających z art. 79 § 2 k.p.a.[29] i rygor natychmiastowej wykonalności decyzji (projektowany art. 67b ust. 18 Ustawy); należy także podzielić uwagę zgłoszoną w toku opiniowania Projektu przez RCL, które zwróciło uwagę, że

> „projektowana regulacja nie zawiera żadnych przesłanek do wszczęcia ww. postępowania. Przesłanki wszczęcia postępowania winny zostać w ustawie dookreślone w taki sposób aby podmioty, wobec których postępowania wszczęto, dysponowały wiedzą o przyczynach wszczęcia tego postępowania, a podmioty, które potencjalnie mogą zostać objęte takim postępowaniem - miały możliwość w ramach prowadzonej przez siebie działalności ocenić, czy sposób w jaki prowadzą tę działalność może skutkować wszczęciem wobec nich postępowania. Tym bardziej, że już samo zamieszczenie informacji o wszczęciu postępowania w Biuletynie Informacji Publicznej może rodzić negatywne skutki dla przedsiębiorcy”[30].

Z punktu widzenia Dyrektywy, ponownie należy zasygnalizować, że taki kształt regulacji, z przyczyn wskazanych w opinii RCL, może równocześnie wywoływać wątpliwości na płaszczyźnie art. 16 w zw. z art. 52 ust. 1 Karty Praw Podstawowych UE;

d) Projektowany art. 67c Ustawy, zakładający obowiązek powstrzymania się od wprowadzania do użytkowania i wycofania z użytkowania produktów dostawy

[27] Zob. wyrok TS z 26 marca 2020 r., C-113/19 *Luxaviation SA v Ministre de l'Environnement*, pkt 47 i powołany tam wyrok TS z 8 maja 2014 r., C-604/12 *H.N. v Minister for Justice, Equality and Law Reform,* pkt 49-50.

[28] Zob. szerzej K. Kowalik-Bańczyk (w:) A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2020, w nb. 34 do art. 41 KPP UE.

[29] Zob. wyłączenie zawarte w projektowanym art. 67b ust. 2 *in fine* Ustawy.

[30] Opinia Rządowego Centrum Legislacji z 23 maja 2024 r., RCL.DISIP.550.5.2024, s. 11.

uznanego za dostawcę wysokiego ryzyka, co może rodzić potencjalnie dewastujące skutkami ekonomiczne decyzji (opatrzonej *ex lege* rygorem natychmiastowej wykonalności);

e) Projektowany art. 67e Ustawy, który zakłada wydanie wyroku, w sprawie ze skargi na decyzję o uznaniu dostawcy za dostawcę wysokiego ryzyka, na posiedzeniu niejawnym, a także ograniczenie treści doręczanego stronie uzasadnienia do tej części, która jest pozbawiona informacji niejawnych, co wzbudza wątpliwości co do zgodności z art. 47 Karty Praw Podstawowych; w tym miejscu należy zaznaczyć, że ograniczenie dostępu dostawy uznanego za dostawcę wysokiego ryzyka do motywów orzeczenia nie budzi wątpliwości co do samej zasady, biorąc pod uwagę względy bezpieczeństwa państwa, jednak w takiej sytuacji należałoby nałożyć na sąd administracyjny obowiązek zrelacjonowania motywów w możliwym zakresie w taki sposób, aby nie ujawnić samych informacji niejawnych; ponadto zaś przepis nie przewiduje terminu instrukcyjnego rozpoznania skargi, co również wzbudza wątpliwości co do proporcjonalności regulacji, biorąc pod uwagę natychmiastową wykonalność decyzji;

f) Ponadto należy w tym miejscu podkreślić, że Dyrektywa oparta jest na założeniu, iż kluczowym elementem systemu cyberbezpieczeństwa są same podmioty kluczowe i ważne. Zgodnie z art. 21 ust. 1 Dyrektywy rolą państw członkowskich jest zapewnienie, że to te podmioty będą „wprowadzały odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych", a same środki będą przez te podmioty określane i stosowane „przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych" oraz przy wzięciu pod uwagę takich okoliczności, jak „stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze". O tym, że dobór środków ma spoczywać zasadniczo na samych podmiotach kluczowych i ważnych, świadczy także treść art. 21 ust. 3 Dyrektywy („państwa członkowskie zapewniają również, aby rozważając, które ze środków, o których mowa w tej literze, są odpowiednie,

podmioty musiały uwzględniać […]"). Patrząc dalej z tej perspektywy należy odnotować wątpliwość co do proporcjonalności omawianej tu regulacji, która zakłada wprowadzenie formuły *high risk vendors* (dostawców wysokiego ryzyka) bez uprzedniego rozważenia parametrów wynikających z art. 21 Dyrektywy, a przesłanki zastosowania tej konstrukcji w ogóle nie zostały w ustawie określone; budzi to wątpliwości, odnoszące się do możliwej arbitralności na etapie aplikacyjnym, z punktu widzenia zgodności regulacji z zasadą proporcjonalności;

g) Projektowany art. 67g Ustawy, dotyczący wydania tzw. polecenia zabezpieczającego w przypadku incydentu krytycznego, który nie określa przesłanej wydania takiego polecenia (nie wydaje się takim określeniem projektowana treść Art. 67g ust. 5 Ustawy, która jest mało precyzyjna i nie konkretyzuje przesłanek), a zarazem umożliwia nałożenie na podmioty kluczowe i ważne bardzo szerokiego i – ponownie – mało precyzyjnego katalogu „obowiązków określonego zachowania" oraz ich utrzymywanie nawet przez okres 2 lat (projektowany art. 67g ust. 12 Ustawy); te elementy konstrukcji projektowanej regulacji wzbudzając wątpliwość co do zgodności z art. 16 i 17 ust. 1 w zw. z art. 52 ust. 1 Karty Praw Podstawowych;

h) Projektowany art. 67i ust. 3 Ustawy, który zakłada wyłączenie możliwości wnioskowania o przywrócenie terminu na złożenie skargi, co wzbudza wątpliwość co do zgodności z art. 47 Karty Praw Podstawowych;

17) Art. 1 pkt 74 Projektu, dotyczący zmian w treści art. 73 Ustawy (administracyjne kary pieniężne), w zakresie, w którym projektowane przepisy:

a) Zakładają rozciągnięcie kar *ratione materiae* również na przypadki naruszenia art. 67c i art. 67g Ustawy w brzmieniu nadanym Projektem – z uwagi na zastosowanie wzbudzającej wątpliwość praktyki stosowania administracyjnych kar pieniężnych o unijnej proweniencji w przypadkach uchybienia obowiązkom nakładanym na jednostki w ramach *gold platingu* transpozycyjnego;

b) Nie zastrzegają zastosowania kary wyższej w przypadku nałożenia kary na podmiot ważny, a kryteria kalkulacji (projektowany art. 73 ust. 4 Ustawy w brzmieniu nadanym Projektem) dawałyby różne rezultaty;

c) Zakładają wprowadzenie nieprecyzyjnych przesłanek zastosowania podwyższonej maksymalnie do 100 mln złotych administracyjnej kary pieniężnej (projektowany art. 73 ust. 5 Ustawy w brzmieniu nadanym Projektem)

   - budzą wątpliwości co do zgodności z art. 17 ust. 1 w zw. z art. 52 ust. 1 Karty Praw Podstawowych oraz z zasadą dobrej administracji;

18) Art. 1 pkt 75 Projektu (dot. dodania projektowanego art. 73a Ustawy), zakładający możliwość stosowania administracyjnych kar pieniężnych w wysokości do 6-rotności wynagrodzenia otrzymywanego przez ukaranego, wobec kierowników podmiotów kluczowych i ważnych – co nie znajduje parcia w treści Dyrektywy (i nie zostało wskazane w odwróconej tabeli zgodności);

19) Art. 1 pkt 76 Projektu, który zakłada w projektowanym brzmieniu art. 74 ust. 2 Ustawy (w brzmieniu nadanym Projektem) nadanie przez organ właściwy rygoru natychmiastowej wykonalności decyzji o nałożeniu kary pieniężnej „jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego" – ponieważ egzekwowanie kar pieniężnych, w przeciwieństwie do egzekwowania obowiązków, których nałożenie zakłada Dyrektywa, nigdy i z natury rzeczy nie wiąże się z potrzebą nałożenia rygoru natychmiastowej wykonalności dla ochrony tych wartości prawnie chronionych, nadto zaś taka konstrukcja wzbudza wątpliwości co do proporcjonalności ingerencji w prawo własności, czyli co do zgodności z art. 17 ust. 1 w zw. z art. 52 ust. 1 Karty Praw Podstawowych;

20) Art. 1 pkt 79 Projektu w zakresie, w jakim dotyczy on możliwości nakładania kar w celu przymuszenia do realizacji czynności określonych w ostrzeżeniu wydanym na podstawie (projektowanego) art. 53 ust 4 Ustawy (w brzmieniu nadanym Projektem), a to z uwagi na wątpliwość co do zgodności z art. 34 ust. 6 Dyrektywy, który uzależnia tę możliwość od wcześniejszego wydania decyzji właściwego organu.

5. Konkluzje ekspertyzy

Przyjęcie ustawy wdrażającej Dyrektywę jest konieczne, bo obowiązek taki wynika z art. 288 TFUE, a termin jego realizacji upływa 17 października 2024 r.[31] Należy jednak zwrócić uwagę na wątpliwości wskazane w cz. 4 niniejszej ekspertyzy i postulować ich rozważenie. Wątpliwości te nie są tego rodzaju, aby nie było możliwe ich wyeliminowanie jeszcze przed skierowaniem Projektu do Sejmu, albo też w toku prac parlamentarnych. Zapewne w jakiejś części ich usunięcie będzie możliwe drogą należytego uzasadnienia, w innej zaś części (zwłaszcza co do treści ujętych w art. 1 pkt 70 – 79 Projektu) poprzez ingerencję w treść Projektu.

Sporządził : r. pr. dr hab. Marcin Górski, prof. UŁ

Łódź, 3 września 2024 r.

[31] Zgodnie z art. 41 Dyrektywy.