Ius Novum

2024, vol. 18, nr 2, s. 102–115

PROJEKT REGULACJI W ZAKRESIE DOSTAWCY WYSOKIEGO RYZYKA

MACIEJ ROGALSKI*

DOI: 10.26399/iusnovum.v18.2.2024.16/m.rogalski

Streszczenie

Przedmiotem artykułu jest wprowadzanie do polskiego porządku prawego uregulowań w zakresie cyberbezpieczeństwa, dotyczących dostawców infrastruktury do świadczenia usług w technologii 5G. W szczególności chodzi o wdrożenie rekomendacji z raportu przygotowanego przez Network and Information System Cooperation Group zatytułowanego Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures („5G Toolbox"). Polska, wykonując zalecenia Komisji Europejskiej, podjęła prace w zakresie wprowadzenia przepisów, które stanowiłyby realizację postanowień 5G Toolbox w zakresie dostawcy wysokiego ryzyka. Przygotowana została nowela ustawy o krajowym systemie cyberbezpieczeństwa z 3 lipca 2023 r. (Projekt), która wprowadza rekomendacje z 5G Toolbox. W artykule zostanie przeprowadzona analiza w celu udzielenia odpowiedzi na pytanie, czy przewidziane w Projekcie przepisy w zakresie postępowania w sprawie tzw. dostawców wysokiego ryzyka są zgodne z Konstytucją oraz podstawowymi zasadami procesowymi, a zwłaszcza czy zostały zapewnione gwarancje prawne dla uczestników postępowania w sprawie dostawców wysokiego ryzyka. Hipotezą badawczą jest twierdzenie, że nie wszystkie projektowane uregulowania w tym zakresie spełniają wskazane wcześniej wymogi. Analiza uwzględniać będzie projektowane regulacje dotyczące: postępowania w sprawie uznanie dostawcy za dostawcę wysokiego ryzyka; stosowanie w tym postępowaniu przepisów Kodeksu postępowania administracyjnego oraz treść wydawanych decyzji i środki odwoławcze. Zastosowana zostanie głównie metoda dogmatyczno-prawna, a także metoda teoretyczno-prawna.

Słowa kluczowe: infrastruktura, dostawca wysokiego ryzyka, cyberbezpieczeństwo, wykluczenie z dostaw

* prof. dr hab., Wydział Prawa i Administracji Uczelni Łazarskiego w Warszawie (Polska), e-mail: m.rogalski@lazarski.edu.pl, ORCID: 0000-0003-4366-642X

REGULATION PROJECT FOR HIGH RISK SUPPLIERS

Abstract
The subject of the article is the introduction into the Polish legal system of cybersecurity regulations regarding infrastructure providers for the provision of 5G technology services. In particular, the implementation of the recommendations from the report prepared by the Network and Information System Cooperation Group entitled Cybersecurity of 5G networks EU Toolbox of risk mitigating measures ("5G Toolbox"). Following the recommendations of the European Commission, Poland has undertaken work to introduce regulations that would implement the provisions of the 5G Toolbox regarding high-risk suppliers. An amendment to the Act on the National Cybersecurity System of July 3, 2023 ("Draft") has been prepared, which includes recommendations from the 5G Toolbox. The article will carry out an analysis in order to answer the question whether the provisions of the Draft regarding proceedings in the case of the so-called high-risk suppliers are consistent with the Constitution and basic procedural principles, and in particular whether legal guarantees have been provided for participants in the proceedings regarding high-risk suppliers. The research hypothesis is that not all proposed regulations in this area meet the previously indicated requirements. The analysis will take into account the proposed regulations regarding: proceedings regarding the recognition of a supplier as a high-risk supplier; application of the provisions of the Code of Administrative Procedure in these proceedings and the content of issued decisions and remedies. Mainly the dogmatic-legal method, as well as the theoretical-legal method, will be used.

Keywords: infrastructure, high risk vendors, cybersecurity, exclusion from deliveries

WSTĘP

W Unii Europejskiej (UE) występuje wiele regulacji, które dotyczą bezpieczeństwa świadczonych usług oraz infrastruktury telekomunikacyjnej. W szczególności wskazać należy dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r., ustanawiającą Europejski Kodeks Łączności Elektronicznej[1] (EKŁE), oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (European Network and Information Security Agency) i certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013[2] (rozporządzenie 2019/881). W UE zostały przyjęte także dokumenty, które odnoszą się bezpośrednio do bezpieczeństwa infrastruktury i usług świadczonych w technologii 5G[3]. W dniu 26 marca 2019 r. Komisja Europejska (KE) przyjęła Zalecenia (UE) 2019/534 w sprawie cyberbezpieczeństwa sieci 5G (zalecenia 2019/534)[4]. NISCG (Network and Information System Cooperation Group) przygotował raport z dnia 9 października 2019 r. EU Coordinated Risk Assessment of the Cybersecurity of 5G

[1] Dz. Urz. UE L nr 321 z 12.12.2019 r., s. 36.
[2] Dz. Urz. UE L nr 151 z 7.06.2019 r., s. 15.
[3] Technologia telefonii mobilnej piątej generacji – standard sieci komórkowej będący następcą standardu 4G.
[4] Dz. Urz. UE L nr 88 z 29.03.2019 r., s. 42–47.

Networks[5], który zawiera analizę zagrożeń dla sieci 5G. W listopadzie 2019 r. ENISA w raporcie Threat Landscape for 5G Networks[6] przedstawiła katalog możliwych zagrożeń dla sieci 5G.

W dniu 29 stycznia 2020 r. został opublikowany raport NISCG przygotowany we współpracy z KE i ENISA Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures (5G Toolbox)[7]. W dokumencie tym określono potencjalne obszary ryzyk w zakresie cyberbezpieczeństwa, w tym ryzyka związane z dostawcami infrastruktury 5G. W szczególności wskazać należy postanowienia zamieszczone w punktach: 2. Supplier-specific vulnerabilities oraz 3. Vulnerabilities stemming from dependency to individual suppliers (s. 42 5G Toolbox). W tabelarycznym zestawieniu ryzyk zawartych w 5G Toolbox chodzi o ryzyka wymienione na s. 35 i oznaczone symbolami SM03 i SM04. Dotyczą one ryzyk związanych z dostarczaniem sprzętu do budowy infrastruktury 5G, pochodzącego od dostawców spoza UE i NATO, w których to ponadto krajach może dochodzić przykładowo do niedemokratycznego wpływu ze strony rządu (władz) na firmy produkujące ten sprzęt, w celu np. pozyskania informacji, które będą przesyłane w ramach świadczenie usług telekomunikacyjnych z wykorzystaniem tego sprzętu w innych krajach, w szczególności UE. 5G Toolbox opisuje także środki zaradcze, które można wdrożyć w celu ograniczenia zidentyfikowanych zagrożeń. W przypadku dostawców sprzętu polegają one na przeprowadzaniu ich weryfikacji na podstawie określonych kryteriów i w razie stwierdzenia, że stanowią oni zagrożenie, podejmowaniu odpowiednich decyzji, w tym możliwości ograniczenia wykorzystywania już posiadanego przez operatorów sprzętu od takich dostawców oraz ograniczenia w przyszłości zakupu sprzętu od tych dostawców. W grudniu 2020 r. KE dokonała przeglądu skutków zalecenia 2019/534, a w szczególności osiągniętych etapów wdrożenia[8]. W wyniku tego przeglądu wskazano w szczególności na potrzebę zapewnienia zbieżnych krajowych rozwiązań w zakresie cyberbezpieczeństa w celu skutecznego ograniczania ryzyka w całej UE[9]. Podobne zalecenia zostały przygotowane także przez ECA (European Court of Auditors) w raporcie ze stycznia 2022 r., gdzie wskazano, że państwa członkowskie zastosowały w praktyce rozbieżne podejścia do stosowania sprzętu od dostawców wysokiego ryzyka[10]. W dniu 15 czerwca 2023 r. został opublikowany przygotowany przez NISCG Second report on Member States' Progress

[5] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 (dostęp: 25.07.2023).

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks (dostęp: 30.08.2023).

[7] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures (dostęp: 25.02.2023).

[8] Commission Report on the Impacts of the Commission Recommendation 2019/534 of 26 March 2019 on the Cybersecurity of 5G Networks, SWD(2020) 357 final, https://data.consilium.europa.eu/doc/document/ST-14354-2020-INIT/en/pdf (dostęp: 14.03.2023).

[9] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020)18, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 (dostęp: 14.01.2023).

[10] Special Report. 5G Roll-out in the EU: Delays in Deployment of Networks with Security Issues Remaining Unresolved, https://www.eca.europa.eu/lists/ecadocuments/sr22_03/sr_security-5g-networks_en.pdf (dostęp: 13.07.2023).

in implementing the EU Toolbox on 5G Cybersecurity, w którym wskazano, że w przypadku braku działań ze strony państw członkowskich we wdrażaniu 5G Toolbox, KE rozważy dalsze działania mające na celu zwiększenie odporności rynku wewnętrznego, w tym zbadanie możliwych ścieżek legislacyjnych[11].

Polska, wykonując zalecenia KE, ENISA i NISCG, podjęła prace w zakresie wprowadzenia do polskiego porządku prawnego przepisów, które stanowiłyby realizację postanowień 5G Toolbox w zakresie dostawcy wysokiego ryzyka. Wdrożenie 5G Toolbox będzie oznaczać wprowadzenie do regulacji krajowych, całkowicie nowych, wcześniej niewystępujących w polskim systemie prawnym rozwiązań. Dokument 5G Toolbox pod względem prawnym posiada charakter wytycznych, zbliżonych, ale nie takich samych, jak wytyczne wydawane np. przez ENISA. Prace legislacyjne nad wdrożeniem 5G Toolbox zostały rozpoczęte jeszcze w 2020 r. i przyjęto, że wprowadzenie wymagań 5G Toolbox nastąpi poprzez nowelę Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (u.k.s.c.)[12]. Przygotowanych zostało w sumie 11 wersji projektu noweli u.k.s.c., a ostatnia, z dnia 3 lipca 2023 r., trafiła do Sejmu (Projekt)[13], ale w dniu 11 września 2023 r. została wycofana przez rząd z dalszych prac sejmowych.

Przedmiotem artykułu będzie kwestia wprowadzenia regulacji 5G Toolbox w zakresie dostawców wysokiego ryzyka do polskiego porządku prawnego z uwzględnieniem Projektu noweli u.k.s.c. z 3 lipca 2023 r. Celem analizy będzie udzielenie odpowiedzi na pytanie, czy przewidziane w Projekcie przepisy w zakresie postępowania w sprawie tzw. dostawców wysokiego ryzyka są zgodne z Konstytucją oraz podstawowymi zasadami procesowymi, a zwłaszcza czy zostały zapewnione gwarancje prawne dla uczestników postępowania w sprawie dostawców wysokiego ryzyka. Konsekwencje wydania decyzji w stosunku do tych dostawców będą bardzo poważne, gdyż prowadzić będą do ograniczenia swobody prowadzenia działalności gospodarczej zarówno przez przedsiębiorców będących dostawcami, jak i operatorów nabywających ich sprzęt. Hipotezą badawczą jest twierdzenie, że nie wszystkie projektowane uregulowania w tym zakresie spełniają wskazane wcześniej wymogi. Analiza uwzględniać będzie projektowane regulacje dotyczące: postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka; stosowania w tym postępowaniu przepisów Kodeksu postępowania administracyjnego oraz treści wydawanych decyzji i środków odwoławczych. Zastosowana zostanie głównie metoda dogmatyczno-prawna, a także metoda teoretyczno-prawna.

---

[11] https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, s. 6, 22, 24 (dostęp: 26.08.2023).

[12] Dz.U. z 2023 r., poz. 913.

[13] Druk sejmowy nr 3745.

POSTĘPOWANIE W SPRAWIE UZNANIA DOSTAWCY ZA DOSTAWCĘ WYSOKIEGO RYZYKA

Istotnym elementem wdrożenia postanowień 5G Toolbox będzie przygotowanie postępowania, które prowadzone będzie w sprawie uznania dostawców sprzętu i oprogramowania do budowy infrastruktury telekomunikacyjnej niezbędnej do świadczenia usług telekomunikacyjnych opartych na technologii 5G za tzw. dostawców wysokiego ryzyka. Przygotowany Projekt noweli u.k.s.c. (art. 1 pkt 60 Projektu) przewidywał w art. 66a postępowanie w sprawie dostawcy wysokiego ryzyka. Zgodnie z art. 66a ust. 1 Projektu minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, mógłby wszcząć z urzędu albo na wniosek przewodniczącego Kolegium[14] postępowanie w sprawie uznania dostawcy[15] produktów ICT[16], usług ICT lub procesów ICT[17], zwanego dalej „dostawcą sprzętu lub oprogramowania", które były wykorzystywane przez podmioty wskazane w tym przepisie – za „dostawcę wysokiego ryzyka".

W kształcie zaproponowanym w Projekcie, postanowienia art. 66a ust. 1 prowadziłyby do ograniczenia swobody prowadzenia działalności gospodarczej, zagwarantowanej nie tylko w art. 2 Ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców[18], ale także w art. 20 Konstytucji RP[19]. Zastosowanie bowiem tych przepisów w praktyce oznaczałoby, że podmiot będący dostawcą sprzętu, których dotychczas mógł ten sprzęt bez ograniczeń sprzedawać, po uznaniu go za dostawcę wysokiego ryzyka nie mógłby go już więcej sprzedawać. Zgodnie bowiem z art. 66b ust. 1 Projektu podmioty, o których mowa w art. 66a ust. 1 Projektu, czyli przykładowo przedsiębiorcy komunikacji elektronicznej, po pierwsze, nie mogliby wprowadzać do użytkowania produktów, usług i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, a po drugie, musieliby wycofać z użytkowania wskazane produkty, usługi i procesy ICT w zakresie objętym decyzją, dostarczane przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia informacji o wspomnianej decyzji (art. 66a ust. 12 Projektu).

W uzasadnieniu do Projektu przywołano art. 22 Konstytucji RP, który dopuszcza ograniczenie wolności działalności gospodarczej w drodze ustawy ze względu na ważny interes publiczny (s. 65 uzasadnienia Projektu)[20] oraz orzecznictwo Trybunału Konstytucyjnego (TK), oparte na art. 22 Konstytucji RP, wskazujące, że

---

[14] Kolegium w rozumieniu art. 4 pkt 20 u.k.s.c., tj. Kolegium do Spraw Cyberbezpieczeństwa.

[15] Pojęcie „dostawcy sprzętu lub programowania" jest zdefiniowane w art. 2 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r., ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającego rozporządzenie (EWG) nr 339/93, Dz. Urz. UE L nr 218 z 13.08.2008 r., s. 30.

[16] Information and Communications Technology (technologie informacyjno-komunikacyjne).

[17] ICT w rozumieniu art. 2 EKŁE.

[18] Dz.U. z 2021 r., poz. 162 ze zm.

[19] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r., nr 78, poz. 483 ze zm.

[20] Strona 65 uzasadnienia Projektu.

wolność działalności gospodarczej nie ma charakteru absolutnego[21]. W doktrynie i orzecznictwie TK wskazuje się jednak, że aby ustanawiane przez organy władzy publicznej ograniczenia wolności działalności gospodarczej były ograniczeniami usprawiedliwionymi (a tym samym by były one konstytucyjnie legalne), muszą być nie tylko ukierunkowane na realizację ważnego interesu publicznego, ale równocześnie muszą też być względem tego ważnego interesu publicznego proporcjonalne[22]. Proporcjonalność ustanawianych ograniczeń jest (obligatoryjną) materialną przesłanką usprawiedliwiającą te ograniczenia, przy czym obowiązek spełniania tej przesłanki przez organy władzy publicznej (kreujące ograniczenia wolności działalności gospodarczej) wynika z art. 31 ust. 3 Konstytucji RP, mówiącego o wymogu „konieczności" ustanawianych ograniczeń[23]. Środki służące do osiągnięcia określonego celu nie mogą być dalej idące niż to, co jest potrzebne dla osiągnięcia tego celu[24]. TK wyjaśniał, *że* zasada proporcjonalności musi być uwzględniana przede wszystkim przy ingerencji prawodawcy w sferę podstawowych praw[25]. Weryfikacja przestrzegania zasady proporcjonalności dokonywana jest z wykorzystaniem odpowiednich testów[26]. W ogólnej ocenie proporcjonalności interwencji należy wziąć pod uwagę, czy: 1) środki zastosowane przez prawodawcę są w stanie doprowadzić do zamierzonych celów; 2) są niezbędne dla ochrony interesu, z którym są powiązane; 3) ich efekty pozostają w proporcji do ciężarów nakładanych na obywatela[27]; 4) czy dostępne są alternatywne i mniej inwazyjne środki; 5) czy dany podmiot otrzyma odszkodowanie z tytułu kosztów i strat powstałych w następstwie interwencji[28].

Przepis art. 66a Projektu w proponowanym kształcie nie spełniał wymogu proporcjonalności i prowadził do naruszenia nakazu równego traktowania podmiotów

---

21 Wyrok TK z 8.04.1998 r., K 10/97, Orzecznictwo Trybunału Konstytucyjnego („OTK") 1998, nr 3, poz. 29; wyrok TK z 10.10.2001 r., K 28/01, OTK 2001, nr 7, poz. 212.

22 Zob. wyrok TK z 25.05.2009 r., SK 54/08, OTK 2009, nr 5, poz. 69.

23 M. Safjan, L. Bosek, *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016, Nb 102–105 do art. 22.

24 S. Wronkowska, *Zarys koncepcji państwa prawnego w polskiej literaturze politycznej i prawnej*, w: eadem, *Polskie dyskusje o państwie prawa*, Warszawa 1995, s. 74. Zob. także wyrok SA w Warszawie z 24.01.2017 r., VI ACa 1587/15, https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/vi-aca-1587-15-podstawa-kontroli-wysokosci-stawek-za-522365773 (dostęp: 28.08.2022).

25 Zob. wyrok TK z 27.04.1999 r., P 7/98, Orzecznictwo Trybunału Konstytucyjnego 1999, nr 4, poz. 72.

26 Wyrok Trybunału Sprawiedliwości UE (TSUE) z 20.08.2007 r. w sprawie Commission v Netherlands, C-279/05, pkt 76. W wyroku z 5.06.2007 r. w sprawie Rosengren, C-170/04, pkt 50. TSUE wskazał, że „to do władz krajowych należy wykazanie, że przepisy krajowe są niezbędne do osiągnięcia zadeklarowanego celu i że celu tego nie można osiągnąć za pomocą mniej dotkliwych zakazów lub ograniczeń". Zob. także wyrok TSUE z 11.09.2008 r. w sprawie Commission v Germany, C-141/07, pkt 50; wyrok z 26.06.1997 r. w sprawie Familiapress, C-368/95, pkt. 27.

27 Zob. wyroki TK z: 9 czerwca 1998 r., K 28/97, OTK 1998, nr 4, poz. 50; 26.04.1999 r., K 33/98, OTK 1999, nr 4, poz. 71; 2.06.1999 r., K 34/98, OTK 1999, nr 5, poz. 94; 21.04.2004 r., K 33/03, OTK-A 2004, nr 4, poz. 31; 27.04.1999 r., P 7/98, OTK 1999, nr 4, poz. 72.

28 Zob. wyrok Europejskiego Trybunału Praw Człowieka (ETPC) z 21.02.1986 r. w sprawie James and others przeciwko United Kingdom, nr skargi 8793/79; wyrok ETPC z 22.02.2005 r. w sprawie Hutten-Czapska przeciwko Polsce, nr skargi 35014/97.

gospodarczych[29]. Przewidywał bowiem najdalej idący środek w postaci wykluczenia określonych podmiotów z rynku, bez poszukiwania jakichkolwiek innych możliwych rozwiązań, zgodnie z zasadą proporcjonalności. Środek nie może być uznany za konieczny, gdyż istnieją mniej restrykcyjne rozwiązania, które pozwalają na osiągnięcie zamierzonego rezultatu. Przykładem takich innych środków może być wezwanie do usunięcia naruszeń lub ograniczenie wykluczenia tylko z dostaw określonego rodzaju produktów czy wykluczenie z określonego obszaru geograficznego.

Przyszłe projektowane przepisy powinny przewidywać także inne środki i rozwiązania, pozwalające na osiągnięcie zamierzonego celu, jakim jest zapewnienie cyberbezpieczeństwa, w inny, mniej radykalny sposób niż wykluczenie konkretnego przedsiębiorcy z rynku dostaw sprzętu telekomunikacyjnego. Wykluczenie dostawcy powinno być środkiem ostatecznym. Projektodawcy powinni także w uzasadnieniu projektowanych przepisów wyjaśnić, dlaczego i w jakim zakresie dobru w postaci zapewnienia bezpieczeństwa mają ustąpić inne dobra, takie jak swoboda prowadzenia działalności gospodarczej. Nie jest bowiem wystarczające ogólne powołanie się na takie zagrożenia, ale konieczne jest przynajmniej wskazanie, jakiego rodzaju są to zagrożenia i dlaczego konieczne jest zastosowanie tak daleko idących środków zaradczych.

STOSOWANIE W POSTĘPOWANIU PRZEPISÓW KODEKSU POSTĘPOWANIA ADMINISTRACYJNEGO

Postępowanie w sprawie uznania dostawcy produktów lub usług ICT za dostawcę wysokiego ryzyka powinno się toczyć na podstawie przepisów Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego[30] (k.p.a.). Projekt przewidywał w art. 66a ust. 2, że stosuje się przepisy k.p.a., ale z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy. Wyłączenie stosowania tych przepisów wywołuje zastrzeżenia. Nie jest przekonywująca argumentacja zawarta w uzasadnieniu Projektu wskazująca w przypadku wyłączenia art. 28 k.p.a. na konieczność usprawnienia przebiegu postępowania (s. 84 uzasadnienia Projektu), a w przypadku wyłączenia stosowania art. 31 k.p.a. na kwestie bezpieczeństwa narodowego (s. 84 uzasadnienie Projektu). Udział organizacji społecznej w postępowaniu może być uzasadniony koniecznością podjęcia ochrony określonych wartości, np. uczciwej konkurencji na danym rynku[31]. Wyłączenie stosowania art. 28 i 31 k.p.a. narusza prawo do korzystania z uprawnień strony oraz prawo do czynnego uczestnictwa w postępowaniu podmiotów, które są adresatami decyzji w sprawie dostawcy wysokiego ryzyka. Wykluczenie stosowania tych przepisów prowadzi do ograniczania prawa do rzetelnego postępowania administracyjnego (art. 8 § 1 k.p.a.),

[29] J. Ciapała, *Konstytucyjna wolność działalności gospodarczej w Rzeczypospolitej Polskiej*, Szczecin 2009, s. 268.

[30] Dz.U. z 2023 r., poz. 775.

[31] Por. B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2022, Nb 2 do art. 31.

w szczególności prawa do uczestniczenia w postępowaniu i obrony swoich praw, które znajdują swoje oparcie w konstytucji RP[32].

Należy także zwrócić uwagę, że przepis art. 66a ust. 3 Projektu definiuje odrębne pojęcie strony na potrzeby tego postępowania. Zgodnie z tym przepisem stroną postępowania jest każdy, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Zdefiniowane w ten sposób pojęcie „strony", przy jednoczesnym wyłączeniu stosowania art. 28 k.p.a., oznacza w praktyce nie tylko ograniczenie, ale wręcz wyłączenie możliwości ochrony swoich praw przez podmioty, które nie spełniają warunków dla uznania za stronę, w rozumieniu art. 66a ust. 3 Projektu. Stroną będzie dostawca wobec którego wszczęto postępowanie. Podmioty wymienione w art. 66a ust. 1 pkty 1–3 Projektu będą związane decyzją wydaną w postępowaniu w sprawie uznania danego dostawcy za dostawcę wysokiego ryzyka, ale nie będą jednak stroną tego postępowania. Podmioty te utracą więc status strony, który posiadałyby, gdyby stosowane były przepisy k.p.a. Sprzeczne jest to ze sposobem kształtowania sytuacji prawnej stron w postępowaniu administracyjnym[33]. Wprawdzie w regulacjach prawnych dotyczących poszczególnych działów gospodarki stosowane są odrębne definicje strony, ale zauważyć należy, że zgodnie z definicją strony w art. 66a ust. 3 Projektu nastąpiło zrównanie pojęcia strony z podmiotem, w stosunku do którego zostało wszczęte postępowanie. W praktyce więc stroną będzie tylko podmiot, który formalnie zostanie wskazany przez organ prowadzący postępowanie jako strona, czyli od niego wyłącznie zależeć będzie to, kto będzie stroną. W ten sposób podmioty zainteresowane udziałem w postępowaniu zostaną pozbawione możliwości ochrony swoich praw, jeżeli organ prowadzący postępowanie uzna, że nie przysługuje im status strony.

Brak statusu strony będzie także wpływać na ocenę interesu prawnego tych podmiotów na podstawie art. 50 Ustawy z dnia z 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (p.p.s.a.)[34]. Następstwem tej oceny może być stwierdzenie braku legitymacji do wniesienia skargi do sądu administracyjnego, czyli pozbawienia tych podmiotów prawa do sądu. Prawo do sądu uznawane jest za prawo podmiotowe[35], przewidziane w art. 45 ust. 1 Konstytucji RP[36]. Przepis art. 77 ust. 2 Konstytucji przewiduje natomiast zakaz zamykania drogi sądowej dochodzenia naruszonych wolności lub praw[37]. Wprawdzie dostęp do drogi sądowej może być

---

[32] Zob. wyrok Wojewódzkiego Sądu Administracyjnego (WSA) z 29.08.2019 r., IV SAB/Po 147/19, Centralna Baza Orzeczeń Sądów Administracyjnych („CBOSA"). Zob. także M. Karpiuk, P. Krzykowski, A. Skóra, *Kodeks postępowania administracyjnego. Komentarz do art. 1–60, Tom I*, Olsztyn 2020, s. 56; T. Majer, *Zasada ogólna współdziałania organów*, w: P. Krzykowski (red.), *Zasady ogólne Kodeksu postępowania administracyjnego*, Olsztyn 2017, s. 49.

[33] Zob. wyrok Naczelnego Sądu Administracyjnego (NSA) w Warszawie z 15.04.1993 r., I SA 1719/92, Orzecznictwo Sądów Polskich (OSP) 1994, z. 10, poz. 199.

[34] Dz.U. z 2002 r., nr 153, poz. 1270 ze zm.

[35] P. Tuleja, *Art. 45*, w: idem (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, wyd. II, Warszawa 2021, SIP LEX.

[36] L. Garlicki, K. Wojtyczek, *Art. 77*, w: L. Garlicki, M. Zubik (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II*, Warszawa 2016, SIP LEX.

[37] Zob. szerzej M. Florczak-Wątor, *Art. 77*, w: P. Tuleja (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, wyd. II, Warszawa 2021, SIP LEX.

ograniczony[38], ale nie może zostać całkowicie wyłączony[39]. Europejski Trybunał Praw Człowieka wyjaśnił, że art. 6 ust. 1 Europejskiej Konwencji Praw Człowieka, przewidujący prawo do sądu, stosuje się także do sprawy administracyjnej, gdy dotyczy ona cywilnoprawnych praw lub obowiązków (w przeważającym zakresie treść lub skutek działania administracji dotyczą sfery majątkowej lub gospodarczej)[40]. Wskazany przepis ma zastosowanie także wtedy, gdy decyzja nie jest bezpośrednio kierowana do danych podmiotów, a jedynie oddziałuje na nie[41]. Sytuacja taka ma miejsce w przypadku podmiotów wskazanych w art. 66a ust. 1 pkty 1–3 Projektu, do których decyzja nie jest skierowana, ale obowiązki z niej wynikające będą ich dotyczyć.

Zastrzeżenia budzi także wyłączenie stosowania art. 79 k.p.a., zapewniającego stronie obecność przy przeprowadzeniu dowodów[42]. W uzasadnieniu Projektu (s. 84) wyjaśniono, że wyłączenie udziału strony z przeprowadzanych dowodów jest konieczne w związku z wrażliwym charakterem informacji, jakie będą wykorzystywane w ramach tego postępowania. Uwzględniając pozostałe wyłączenia przepisów k.p.a., strona uczestnicząca w tym postępowaniu w praktyce zostanie pozbawiona jednak realnego wpływu na przebieg tego postępowania. Nawet względy bezpieczeństwa państwowego nie mogą uzasadniać pozbawienia strony wynikającego z Konstytucji prawa do obrony. W praktyce, oczywiście, mogą pojawić się okoliczności uzasadniające wyłączenie jawności określonych informacji czy czynności. Wyłączenie udziału strony w czynnościach dowodowych powinno być jednak ograniczone do tych informacji czy czynności, a nie posiadać charakter generalnego wyłączenia od udziału we wszystkich czynnościach dowodowych prowadzonych w tym postępowaniu.

Projektodawcy przewidzieli także uregulowanie, które przynajmniej częściowo ma rozwiązywać problem wyłączenia stosowania art. 28 k.p.k. Zgodnie więc z art. 66a ust. 4 Projektu do postępowania może przystąpić, na wniosek, na prawach strony, przedsiębiorca telekomunikacyjny, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego[43]. Propozycja ta, zamiast rozwiązać problem wyłączenia stosowania art. 28 i 31 k.p.a., wywołuje jednak dodatkowo inne problemy. Przepis art. 66a ust. 4 Projektu różnicuje bowiem sytuację prawną przedsiębiorców

---

[38] Por. wyrok TK z 14.11.2006 r., SK 41/04, OTK 2006, nr 10/A, poz. 150.

[39] Por. L. Garlicki, K. Wojtyczek, *Art. 77…*, op. cit. i przytaczane tam wyroki TK z: 16.03.1999 r., SK 19/98; 14.06.1999 r., K 11/98; 10.05.2000 r., K 21/00; 15.06.2004 r., SK 43/03; 12.10.2004 r., P 22/03; 14.03.2005 r., K 35/04.

[40] Por. P. Hofmański, A. Wróbel, *Artykuł 6*, w: L. Garlicki (red.), *Konwencja o ochronie praw człowieka i podstawowych wolności. Tom I. Komentarz do artykułów 1–18*, Warszawa 2010, SIP Legalis, pkty 36–37 i przytaczane tam wyroki ETPC.

[41] Por. wyrok ETPC z 6.04.2000 r. w sprawie Athanassoglou i inni v. Szwajcaria, nr skargi 27644/95, pkt 45.

[42] Zob. R. Hauser, M. Wierzbowski, *Kodeks postępowania karnego. Komentarz*, Warszawa 2023, Nb 1 do art. 79.

[43] Komunikat Prezesa Głównego Urzędu Statystycznego o którym mowa w art. 20 pkt 1 lit. a Ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U. z 2022 r., poz. 504, 1504 i 2461).

telekomunikacyjnych. W postępowaniu będą mogli wziąć udział jedynie najwięksi przedsiębiorcy, tj. ci, których przychód wyniósł ponad 102 miliony zł. Z uzasadnienia Projektu wynika, że tylko 69 przedsiębiorców telekomunikacyjnych przekroczyło w ogóle kwotę 10 mln przychodów, która to kwota jest graniczną w zakresie konieczności przygotowania planu na wypadek szczególnych zagrożeń[44] (s. 88 uzasadnienia Projektu). Z raportu Urzędu Komunikacji Elektronicznej (UKE)[45] wynika natomiast, że w 2022 r. było 3900 przedsiębiorców telekomunikacyjnych. Ogromna więc większość przedsiębiorców telekomunikacyjnych będzie wykluczona z postępowania w sprawie dostawcy wysokiego ryzyka. Natomiast wynik tego postępowania będzie miał wpływ na wszystkich przedsiębiorców, bez względu na osiągnięty przychód z tytułu prowadzenia działalności telekomunikacyjnej, gdyż każdy przedsiębiorca może zostać objęty obowiązkiem wycofania sprzętu z użytkowania, bez względu na wysokość osiągniętego przychodu. Uregulowania te mogą więc zostać uznane za naruszające zasadę równości wobec prawa wyrażoną w art. 32 ust. 1 Konstytucji RP[46]. W przypadku zróżnicowania sytuacji prawnej pomiotów według określonego kryterium, musi spełniać ono katalog określonych warunków, które wskazuje wyrok TK z 28 marca 2007 r., K 40/04[47]. Przepis art. 66a ust. 4 Projektu nie uwzględnia jednak żadnego z trzech kryteriów wskazanych w tym wyroku. Projektowane przepisy nie powinny więc wykluczać z postępowania przedsiębiorców tylko dlatego, że osiągają mniejsze przychody, ale umożliwić każdemu z nich, gdy będą zainteresowani, udział w tym postępowaniu, gdyż na ich prawa i obowiązki będzie oddziaływać wynik tego postępowania.

TREŚĆ WYDAWANYCH DECYZJI I ŚRODKI ODWOŁAWCZE

Zgodnie z art. 66a ust. 12 Projektu treścią wydawanej przez ministra właściwego do spraw informatyzacji decyzji byłoby uznanie dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowiłby poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. Według art. 66a ust. 15 Projektu decyzja ta podlegać miała natychmiastowemu wykonaniu. Wykonalność tej decyzji mogła zostać wstrzymana na podstawie art. 61 § 3 p.p.s.a., regulującym instytucję tzw. ochrony tymczasowej w postępowaniu sądowoadministracyjnym[48], której celem jej jest

---

[44] Zob. § 2 ust. 1 pkt 1 rozporządzenia Rady Ministrów z dnia 19 sierpnia 2020 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz.U. z 2020 r., poz. 1464).

[45] Raport o stanie rynku telekomunikacyjnego w 2022 r., Urząd Komunikacji Elektronicznej, czerwiec 2023 r., file:///C:/Users/macie/Downloads/uke_raport_tele_2022_2-1.pdf (dostęp: 7.10.2023).

[46] P. Tuleja, W. Wróbel, *Zasada równości w stanowieniu prawa*, w: H. Rot (red.), *Demokratyczne państwo prawne (aksjologia, struktura, funkcje). Studia i szkice*, Wrocław 1992, s. 139.

[47] OTK-A 2007, nr 3, poz. 33, Nb 40.

[48] P. Daniel, *Ochrona tymczasowa w przepisach p.p.s.a. w świetle prawa unijnego*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2011, nr 5, s. 36 i n.

ochrona strony skarżącej przed skutkami wykonania zaskarżonej decyzji, które mogą być trudne do odwrócenia, po ewentualnym jej uchyleniu przez sąd[49].

Zgodnie z art. 66a ust. 16 Projektu od tej decyzji nie przysługiwałby wniosek o ponowne rozpatrzenie sprawy. Nie byłoby więc możliwe zaskarżenie decyzji o uznaniu za dostawcę wysokiego ryzyka w ramach postępowania administracyjnego. Według natomiast art. 78 Konstytucji RP do praw podmiotowych zalicza się możliwość zaskarżenia decyzji administracyjnej wydanej w pierwszej instancji. Dotyczy to także wniosku o ponowne rozpatrzenie sprawy[50]. Przepis art. 78 Konstytucji RP przewiduje wprawdzie wyjątki, ale nie oznacza to dla ustawodawcy niczym nieskrępowanej swobody w określaniu takich wyjątków, a odstępstwo od tej zasady musi być usprawiedliwione szczególnymi okolicznościami, które usprawiedliwiałyby pozbawienie strony tego środka odwoławczego, a ponadto musi być zgodne m.in. z wspomnianą już zasadą proporcjonalności (art. 31 ust. 3 Konstytucji)[51].

Od decyzji przysługiwałaby natomiast skarga do sądu administracyjnego. Zgodnie jednak z art. 66d ust. 1 Projektu skarga rozpatrywana byłaby przez sąd na posiedzeniu niejawnym w składzie trzech sędziów. W uzasadnieniu Projektu (s. 92) wyjaśniono, że przewidziane w art. 66d przepisy dotyczące procedury przed sądem administracyjnym są przepisami o charakterze *lex specialis* do p.p.s.a. oraz że przepis ten jest wzorowany na art. 38 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[52]. Prawo do sądu może być jednak ograniczone tylko zgodnie z wymogami art. 31 ust. 3 Konstytucji. Nie można zastąpić testu zgodności z tymi wymogami poprzez odwołanie się na zasadzie analogii do innych przepisów. Przepis art. 66d ust. 1 Projektu naruszał postanowienia art. 45 ust. 1 Konstytucji RP, przewidującego jawność wewnętrzną, która wymaga zapewnienia stronie postępowania pełnoprawnego udziału w tym postępowaniu[53]. Naruszał także art. 47 Karty Praw Podstawowych UE[54] (Karta) i art. 6 Europejskiej Konwencji Praw Człowieka[55] (EKPC), które również gwarantują każdemu prawo do jawnego rozpoznanie sprawy przez sąd.

Z kolei zgodnie z art. 66d ust. 2 Projektu odpis sentencji wyroku z uzasadnieniem miał być doręczany wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręczany byłby odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych. Przepis art. 66a ust. 2 zd. 2 Projektu także naruszał postanowienia art. 45 Konstytucji RP i art. 6 ust. 1 EKPC, gwarantujące każdemu prawo do sądu, gdyż przewidywał doręczenie skarżącemu tylko części uzasadnienia wyroku[56]. Trafnie w swojej opinii

---

[49] Zob. postanowienie NSA z 29.05.2015 r., II GZ 251/15, Legalis nr 1386368; postanowienie WSA w Poznaniu z 25.06.2019 r., IV SA/Po 425/19, Legalis nr 1948826.

[50] Por. wyrok TK z 25.07.2013 r., SK 61/12, OTK-A 2013, nr 6, poz. 85, Nb 115.

[51] Wyrok TK z 12.06.2002 r., P 13/01, OTK ZU 2002, nr 4/A, poz. 42.

[52] Dz.U. z 2019 r., poz. 742, z późn. zm.

[53] Zob. wyrok TK z 6.12.2004 r., SK 29/04, OTK-A 2004, nr 11, poz. 114, Nb 51.

[54] Dz. Urz. UE C 202/02 z 7.06.2016 r., s. 393.

[55] Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami Nr 3, 5 i 8 oraz uzupełniona Protokołem Nr 2 (Dz.U. z 1993 r., nr 61, poz. 284 ze zm.).

[56] Zob. wyrok ETPC z 18.12.1984 r. w sprawie Sporrong i Lönnroth przeciwko Szwecji, nr skargi 7151/75; wyrok TSUE z 1.07.2008 r. w sprawie Chronopost SA i La Poste przeciwko Union Française de L'express (UFEX) i in., C-341/06 P i C-342/06 P, ECLI:EU:C:2008:375, pkty 44 i 45.

Rada Legislacyjna zauważyła, że wyrok sądu administracyjnego musi w świetle konstytucyjnego prawa do sądu zawierać pełne uzasadnienie doręczane stronie, gdyż na podstawie tego uzasadnienia strona może skutecznie wykorzystać swoje uprawnienia do zaskarżenia tego wyroku na drodze sądowej. Rada nie negowała, że w przypadku postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, względy obronności i bezpieczeństwa państwa (art. 31 ust. 3 Konstytucji RP) są aktualne. Natomiast miała wątpliwości, czy zastosowane w tym zakresie rozwiązanie prawne, polegające na ograniczeniu możliwości poznania przez stronę uzasadnienia faktycznego decyzji administracyjnej i uzasadnienia wyroku sądu administracyjnego, są proporcjonalne[57].

Zasada proporcjonalności oznacza bowiem takie treściowe ukształtowanie regulacji prawnej, aby zachowane zostały odpowiednio wyważone proporcje pomiędzy – z jednej strony – konstytucyjnymi wartościami usprawiedliwiającymi ingerencję, a – z drugiej – stopniem ingerencji w dane konstytucyjne prawo lub wolność i związanej z tym uciążliwości[58]. W doktrynie zostały wypracowane kryteria, które są pomocne dla oceny uciążliwości środków ingerencyjnych, do których zaliczają się: zakres przedmiotowy ingerencji, zakres podmiotowy ingerencji, zakres przestrzenny ingerencji oraz zakres czasowy ingerencji[59]. W orzecznictwie TK podkreśla się, że jeżeli zakres ograniczeń danego konstytucyjnego prawa lub wolności przybierze taki rozmiar, że dojdzie do „zniweczenia" podstawowych składników danego konstytucyjnego prawa, do „wydrążenia ich z rzeczywistej treści" i „przekształcenia ich w pozór" tego prawa, to wówczas naruszona zostanie podstawowa treść („istota") danego konstytucyjnego prawa, co jest konstytucyjnie niedopuszczalne[60]. Tego rodzaju sytuacja powstanie w przypadku dostawcy, który zostanie uznany za dostawcę wysokiego ryzyka. Podmiot ten został pozbawiony narzędzi prawnych, umożliwiających mu wszczęcie kontroli instancyjnej na etapie postępowania administracyjnego. Projekt ograniczył mu możliwość udziału w rozprawie przed sądem administracyjnym, który dokonuje oceny prawidłowości przeprowadzonego postępowania. Pozbawiony został także możliwości zapoznania się z całością uzasadnienia wyroku sądu administracyjnego. Ponadto Projekt przewidywał natychmiastową wykonalność decyzji z mocy prawa. Wszystkie te ograniczenia zastosowane łącznie powodowały, że nie mogły być uznane za zgodne z Konstytucją i za proporcjonalne *sensu stricto*, jako służące bezpieczeństwu państwa.

---

[57] Zob. pkt 7 opinii Rady Legislacyjnej z dnia 23 lutego 2021 r. do noweli ustawy o Krajowym systemie cyberbezpieczeństwa, https://www.gov.pl/web/radalegislacyjna/opinia-z-23-lutego-2021-r-o-projekcie-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy--prawo-telekomunikacyjne (dostęp: 20.10.2022).

[58] M. Safjan, L. Bosek (red.), *Kosntytucja RP. Tom I. Komentarz do art. 1–86,* Warszawa 2016, Nb 122 do art. 31.

[59] M. Szydło, *Wolność działalności gospodarczej jako prawo podstawowe*, Bydgoszcz–Wrocław 2011, s. 212–216; D. Kijowski, *Zasada adekwatności w prawie administracyjnym*, „Państwo i Prawo" 1990, nr 4, s. 62; idem, *Pozwolenia w administracji publicznej. Studium z teorii prawa administracyjnego*, Białystok 2000, s. 251–252; K. Wojtyczek, *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999, s. 159.

[60] Wyrok TK z 12.01.2000 r., P 11/98, OTK 2000, nr 1, poz. 3.

PODSUMOWANIE

Projekt noweli u.k.s.c. z 3 lipca 2023 r. zawierał postanowienia, które mogłyby zostać uznane za niezgodne z Konstytucją RP oraz podstawowymi zasadami prawa procesowego, w szczególności w zakresie zapewnienia gwarancji prawnych dla uczestników postępowania w sprawie dostawców wysokiego ryzyka. Postanowienia art. 66a ust. 1 Projektu przewidywały ograniczenie swobody prowadzenia działalności gospodarczej, na co zezwala art. 22 Konstytucji RP, pod warunkiem, że ograniczenia te są ukierunkowane na realizację ważnego interesu publicznego i równocześnie są względem tego interesu publicznego proporcjonalne (art. 31 ust. 3 Konstytucji RP). Środki służące do osiągnięcia określonego celu nie mogą być dalej idące niż to, co jest potrzebne dla osiągniecia tego celu. Projekt nie przewidywał natomiast innych, alternatywnych, mniej restrykcyjnych środków niż wprowadzenie w praktyce zakazu prowadzenia działalności dla danego podmiotu. Środkami tymi mogłyby być: ograniczenie wymogów tylko do określonego rodzajów produktów lub wprowadzenie geograficznie określonych ograniczeń. W przewidzianym w Projekcie kształcie, przepis art. 66a Projektu nie spełnia więc wymogu proporcjonalności.

Poważne zastrzeżenia wywołuje także wyłączenie stosowania art. 28, 31 i 79 k.p.a. w postępowaniu w sprawie dostawcy wysokiego ryzyka. Wyłączenie stosowania art. 28 i 31 k.p.a. narusza prawo do korzystania z uprawnień strony oraz prawo do czynnego udziału w postępowaniu podmiotów, które są adresatami decyzji w sprawie dostawcy wysokiego ryzyka. Z kolei wyłączenie udziału strony w czynnościach dowodowych (art. 79 k.p.a.) powinno być ograniczone tylko do określonych czynności, a nie posiadać charakter generalnego wyłączenia od udziału we wszystkich czynnościach dowodowych prowadzonych w tym postępowaniu. Uwzględniając pozostałe wyłączenia przepisów k.p.a., strona uczestnicząca w tym postępowaniu w praktyce zostanie pozbawiona realnego wpływu na przebieg tego postępowania.

Zdefiniowane w art. 66a ust. 3 Projektu pojęcie strony, przy jednoczesnym wyłączeniu stosowania art. 28 k.p.a., oznacza w praktyce ograniczenie możliwości ochrony swoich praw przez podmioty, które nie spełniają warunków dla uznania za stronę, w rozumieniu tego przepisu, ale będą związane decyzją wydaną w tym postępowaniu. Podmioty wskazane w art. 66a ust. 1 pkty 1–3 Projektu utracą więc status strony, który posiadałyby, gdyby stosowane były przepisy k.p.a. W praktyce więc stroną będzie tylko podmiot, który formalnie zostanie wskazany przez organ prowadzący postępowanie jako strona, czyli od niego wyłącznie zależeć będzie, kto będzie stroną. Sprzeczne jest to ze sposobem kształtowania sytuacji prawnej stron w postępowaniu administracyjnym.

Przepis art. 66a ust. 2 zd. 2 Projektu narusza postanowienia art. 45 Konstytucji RP i art. 6 ust. 1 EKPC, gwarantujące każdemu prawo do sądu, gdyż przewiduje doręczenie skarżącemu tylko część uzasadnienia wyroku. Wyrok sądu administracyjnego musi zawierać pełne uzasadnienie doręczane stronie, gdyż dopiero na podstawie tego uzasadnienia strona może skutecznie wykorzystać swoje uprawnienia do zaskarżenia tego wyroku na drodze sądowej. Zastosowane w tym zakresie rozwiązania prawne, polegające na ograniczeniu możliwości poznania przez stronę uzasadnienia faktycznego decyzji administracyjnej i uzasadnienia wyroku sądu administracyjnego, są nieproporcjonalne.

Przygotowana nowa wersja zmian do ustawy o krajowym systemie cyberbezpieczeństwa, przewidująca uregulowania w zakresie dostawców wysokiego ryzyka, powinna wyeliminować dotychczasowe opisane wady Projektu, w celu zapewnienia jego zgodności z postanowieniami Konstytucji oraz z podstawowymi zasadami procesowymi.

BIBLIOGRAFIA

Adamiak B., Borkowski J., *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2022.

Ciapała J., *Konstytucyjna wolność działalności gospodarczej w Rzeczypospolitej Polskiej*, Szczecin 2009.

Daniel P., *Ochrona tymczasowa w przepisach p.p.s.a. w świetle prawa unijnego*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2011, nr 5.

Florczak-Wątor M., *Art. 77*, w: P. Tuleja (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2021.

Garlicki L., Wojtyczek K., *Art. 77*, w: L. Garlicki, M. Zubik (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom II*, Warszawa 2016.

Hauser R., Wierzbowski M., *Kodeks postępowania karnego. Komentarz*, Warszawa 2023.

Hofmański P., Wróbel A., *Artykuł 6*, w: L. Garlicki (red.), *Konwencja o ochronie praw człowieka i podstawowych wolności. Tom I. Komentarz do artykułów 1–18*, Warszawa 2010.

Karpiuk M., Krzykowski P., Skóra A., *Kodeks postępowania administracyjnego. Komentarz do art. 1–60, Tom I*, Olsztyn 2020.

Kijowski D., *Pozwolenia w administracji publicznej. Studium z teorii prawa administracyjnego*, Białystok 2000.

Kijowski D., *Zasada adekwatności w prawie administracyjnym*, „Państwo i Prawo" 1990, nr 4.

Majer T., *Zasada ogólna współdziałania organów*, w: P. Krzykowski (red.), *Zasady ogólne Kodeksu postępowania administracyjnego*, Olsztyn 2017.

Safjan M., Bosek L., *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016.

Szydło M., *Wolność działalności gospodarczej jako prawo podstawowe*, Bydgoszcz–Wrocław 2011.

Tuleja P., *Art. 45*, w: idem (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2021.

Tuleja P., Wróbel W., *Zasada równości w stanowieniu prawa*, w: H. Rot (red.), *Demokratyczne państwo prawne (aksjologia, struktura, funkcje). Studia i szkice*, Wrocław 1992.

Wojtyczek K., *Granice ingerencji ustawodawczej w sferę praw człowieka w Konstytucji RP*, Kraków 1999.

Wronkowska S., *Zarys koncepcji państwa prawnego w polskiej literaturze politycznej i prawnej*, w: eadem, *Polskie dyskusje o państwie prawa*, Warszawa 1995.

Cytuj jako:

Rogalski M., *Projekt regulacji w zakresie dostawcy wysokiego ryzyka*, „Ius Novum" 2024, nr 2 (18), s. 102–115. DOI: 10.26399/iusnovum.v18.2.2024.16/m.rogalski