Mariusz Czyżak*

Odpowiedzialność karnoadministracyjna kierownika operatora usługi kluczowej za niezachowanie należytej staranności

Spis treści

Streszczenie

W artykule omówiono kwestię odpowiedzialność kierownika operatora usług kluczowych za naruszenie obowiązku dochowania należytej staranności przy wykonywaniu obowiązków przez operatora. Obowiązki te obejmują wdrożenie systemu zarządzania bezpieczeństwem w systemie informatycznym służącym do świadczenia usługi kluczowej, wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz zapewnienie prowadzenia audytów bezpieczeństwa systemu informatycznego wykorzystywanego do świadczenia usługi kluczowej. Za kierownika operatora usługi kluczowej uznać można osobę, która osobę zarządzającą lub współzarządzającą operatorem usługi kluczowej, w szczególności członka organu zarządzającego (zarządu). Odpowiedzialność zarządcy jest odpowiedzialnością odrębną od odpowiedzialności operatora usługi kluczowej. Zgodnie z poglądami doktryny i orzecznictwa zachowanie należytej staranności wymaga profesjonalizmu i sumienności. Organ ds. cyberbezpieczeństwa nakłada karę pieniężną za niezachowanie należytej staranności, kierując się wytycznymi zawartymi w Kodeksie postępowania administracyjnego. W artykule przedstawiono również wnioski de lege ferenda, w tym propozycję przeznaczenia środków z kary pieniężnej na Fundusz Cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo; kara pieniężna; operator usługi kluczowej.

JEL: K23, K24, K32, K42

* Dr nauk prawnych, adiunkt, Wydział Administracji, Wyższa Szkoła Kadr Menedżerskich, Konin. ORCID: https://orcid.org/0000-0003-0869-3713.

Edition of that article was financed under Agreement Nr RCN/SP/0326/2021/1 with funds from the Ministry of Education and Science, allocated to the “Rozwoj czasopism naukowych” programme.

internetowy Kwartalnik Antymonopolowy i Regulacyjny 2023, nr 4(12), 84–..... • ISSN 2299-5749 • DOI: 10.7172/2299-5749.IKAR.4.12.XX • www.ikar.wz.uw.edu.pl

I. Wprowadzenie

Przedmiotem regulacji ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1] (dalej: ustawa o ksc lub uksc) jest w szczególności organizacja krajowego systemu cyberbezpieczeństwa, którego celem jest „zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów" oraz zadania i obowiązki podmiotów, które wchodzą w jego skład, jak również sposób sprawowania nadzoru i kontroli w zakresie wykonywania przepisów ustawy o krajowym systemie cyberbezpieczeństwa (art. 1 i 3 ustawy o ksc). W skład systemu cyberbezpieczeństwa wchodzą podmioty posiadające status operatora usług kluczowych. Niewywiązywanie się z niektórych powinności spoczywających na tej kategorii podmiotów skutkuje poniesieniem przez nie odpowiedzialności karnoadministracyjnej. Współczesny ustawodawca coraz częściej korzysta bowiem z kar pieniężnych, uznając je za skuteczne narzędzie regulacyjne stosowane przez organy sprawujące nadzór w różnych obszarach funkcjonowania państwa (Crafoord i Nykvist, 2021, s. 902). W myśl postanowień art. 75 ustawy o ksc, „organ właściwy do spraw cyberbezpieczeństwa może nałożyć karę pieniężną na kierownika operatora usługi kluczowej w przypadku, gdy nie dochował należytej staranności celem spełnienia obowiązków, o których mowa w art. 8 pkt 1, art. 9 ust. 1 pkt 1 oraz art. 15 ust. 1 [ustawy o ksc – M.Cz.], z tym że kara ta może być wymierzona w kwocie nie większej niż 200% jego miesięcznego wynagrodzenia". Przedmiotem dalszych rozważań stanie się analiza znamion przywołanego powyżej deliktu administracyjnego.

II. Pojęcie „kierownika operatora usługi kluczowej"

Przed podjęciem rozważań nad istotą wspomnianego powyżej deliktu administracyjnego przybliżyć należy zatem znaczenie takich pojęć, jak „usługa kluczowa", „operator usługi kluczowej" oraz „kierownik operatora usługi kluczowej".

W przypadku dwóch pierwszych terminów nie sposób nie przywołać ich definicji ustawowej sformułowanej na gruncie ustawy o krajowym systemie cyberbezpieczeństwa. Usługą kluczową jest zatem usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej bądź gospodarczej, wymieniona w wykazie usług kluczowych (art. 2 pkt 16 ustawy o ksc). Operatorem usługi kluczowej jest natomiast podmiot, o którym mowa w załączniku nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa, który posiada jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, a organ właściwy do spraw cyberbezpieczeństwa wydał wobec niego decyzję o uznaniu za operatora usługi kluczowej. Organ ten wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej, jeśli świadczy on usługę kluczową, jej świadczenie zależy od systemów informacyjnych, a incydent (zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo) miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora (art. 5 ustawy o ksc).

Do kategorii operatorów usługi kluczowej należą przykładowo podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji; przedsiębiorstwo

[1] Ustawa z dn. 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2023 poz. 913).

energetyczne posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej; podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej; zarządzający lotniskiem; przewoźnik kolejowy, którego działalność podlega licencjonowaniu; armator; podmiot leczniczy; bank krajowy; przedsiębiorstwo wodociągowo-kanalizacyjne; podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD) (załącznik nr 1 do uksc). Zgodnie z art. 7 ust. 1 ustawy o ksc minister właściwy do spraw informatyzacji prowadzi wykaz operatorów usług kluczowych. Wpisu do niego (i wykreślenia) dokonuje się na wniosek organu właściwego do spraw cyberbezpieczeństwa, złożony niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej (art. 7 ust. 3 ustawy o ksc). Wykaz usług kluczowych określony został w rozporządzeniu Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[2]. Należą do nich np. wydobywanie węgla kamiennego; usługi systemowe, jakościowe i zarządzanie infrastrukturą energetyczną; transport kolejowy pasażerski i towarów; transport lotniczy pasażerski i towarów; obrót ciepłem; przyjmowanie depozytów pieniężnych lub innych funduszy podlegających zwrotowi od klientów; obrót energią elektryczną; obrót i dystrybucja produktów leczniczych; dostarczanie wody; prowadzenie autorytatywnego serwera DNS.

Samego pojęcia „kierownika operatora usługi kluczowej" ustawodawca jednak nie wyjaśnił. W znaczeniu potocznym kierownikiem *jest „osoba zarządzająca jakimś działem, zespołem ludzi"* (Sobol, 2006, s. 319), a zatem, jak się wydaje, kierownik operatora usługi kluczowej, który może przybrać formę prawną różnej kategorii, to osoba pełniąca funkcje zarządcze samodzielnie lub kolegialnie w określonym podmiocie zbiorowym. Ustawodawca, określając status prawny i zasady funkcjonowania tego rodzaju podmiotów, a także nakładając na nie pewne obowiązki ustawowe, w różny sposób i w różnym kontekście określa także nazwy i skład ich organów zarządzających i nadzorczych. W literaturze (np. Kitler, Taczkowska-Olszewska i Radoniewicz, 2019, art. 75, t. 1; Czaplicki, Gryszczyńska i Szpor, 2019, art. 75, t. 4) spotkać się można np. z poglądem o zasadności zastosowania do wyjaśnienia zakresu pojęciowego sformułowania „kierownik operatora usługi kluczowej" definicji legalnej „kierownika jednostki", z którą możemy się spotkać na gruncie ustawy z dnia 29 września1994 r. o rachunkowości[3]. Jej przepis art. 3 ust. 1 pkt 6 stanowi, że status ten posiada w szczególności:

– członek zarządu lub innego organu zarządzającego, a jeżeli organ jest wieloosobowy – członkowie tego organu, z wyłączeniem pełnomocników ustanowionych przez jednostkę;
– w przypadku spółki jawnej i spółki cywilnej – wspólnicy prowadzący sprawy spółki;
– w przypadku spółki partnerskiej – wspólnicy prowadzący sprawy spółki albo zarząd,
– w przypadku spółki komandytowej i spółki komandytowo-akcyjnej – komplementariusze prowadzący sprawy spółki;
– w przypadku osoby fizycznej prowadzącej działalność gospodarczą – ta osoba;

[2] Rozporządzenie Rady Ministrów z dn. 11.09.2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. 2018 poz. 1806).

[3] Ustawa z dn. 29.09.1994 r. o rachunkowości (Dz. U. 2023 poz. 120, ze zm.).

– likwidator, syndyk lub zarządca ustanowiony w postępowaniu restrukturyzacyjnym oraz zarządca sukcesyjny, o którym mowa w ustawie z dnia 5 lipca 2018 r. o zarządzie sukcesyjnym przedsiębiorstwem osoby fizycznej i innych ułatwieniach związanych z sukcesją przedsiębiorstw[4].

Pojęciem „kierownika" ustawodawca posługuje się również na gruncie niektórych aktów normatywnych, w szczególności tych, które regulują sposób wynagradzania osób zajmujących stanowiska kierownicze w podmiotach należących do szeroko rozumianego sektora publicznego. Artykuł 2 pkt 1 ustawy z dnia 3 marca 2000 r. o wynagrodzeniu osób kierujących niektórymi podmiotami prawnymi[5], do kierowników takich jednostek organizacyjnych, jak np. przedsiębiorstwa państwowe, państwowe jednostki organizacyjne posiadające osobowość prawną, samorządowe jednostki organizacyjne posiadające osobowość prawną i niebędące spółkami handlowymi, agencje państwowe, instytuty badawcze, fundacje, państwowe jednostki budżetowe, zalicza m.in. dyrektorów, prezesów, tymczasowych kierowników, zarządców komisarycznych i osoby zarządzające na podstawie umów cywilnoprawnych. W art. 1 ust. 3 pkt 2 ustawy z dnia 9 czerwca 2016 r. o zasadach kształtowania wynagrodzeń osób kierujących niektórymi spółkami[6] mamy z kolei do czynienia z pojęciem „członka organu zarządzającego", które obejmuje członka zarządu spółki kapitałowej, dyrektora w prostej spółce akcyjnej, członka rady administrującej uprawnionego do prowadzenia spraw spółki europejskiej oraz likwidatora. Przytoczyć wypada również przepis art. 126 ust. 6 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe[7], gdzie mowa jest o takich osobach kierujących jednostką, jak „osoba fizyczna będąca przedsiębiorcą, członek zarządu spółki prawa handlowego, dyrektor przedsiębiorstwa, wspólnik spółki jawnej, komplementariusz w spółce komandytowej lub komandytowo-akcyjnej", które ponoszą odpowiedzialność karnoadministracyjną, w sytuacji, gdy podległa im „jednostka kontrolowana uniemożliwia lub utrudnia przeprowadzenie kontroli, mimo powiadomienia przez kontrolującego tej osoby o kontroli".

Jakkolwiek materia przywołanych powyżej ustaw odbiega zasadniczo od przedmiotu regulacji ustawy o krajowym systemie cyberbezpieczeństwa, to przyjęty na ich gruncie punkt widzenia ustawodawcy co do kręgu osób pełniących w określonych podmiotach funkcje, którym można przypisać charakter kierowniczy, okazać może się pomocny dla zdefiniowania pojęcia „kierownika podmiotu zbiorowego", w szczególności „kierownika operatora usługi kluczowej". Wydaje się, że w świetle powyższego za kierownika operatora usługi kluczowej uznać można zatem osobę zarządzającą (współzarządzającą) operatorem usługi kluczowej, w szczególności członka organu zarządzającego (zarządu). Nie będzie nim natomiast osoba będąca członkiem organu nadzorczego (np. rady nadzorczej) w podmiocie posiadającym status operatora usługi kluczowej, a także osoba zajmująca w nim stanowisko kierownicze średniego lub niższego szczebla ani pełnomocnik ustanowiony przez kierownika tego podmiotu, niezależnie od zakresu posiadanego pełnomocnictwa.

[4] Ustawa z dn. 5.07.2018 r. o zarządzie sukcesyjnym przedsiębiorstwem osoby fizycznej i innych ułatwieniach związanych z sukcesją przedsiębiorstw (Dz. U. 2021 poz. 170).

[5] Ustawa z dn. 3.03.2000 r. o wynagrodzeniu osób kierujących niektórymi podmiotami prawnymi (Dz. U. 2019 poz. 2136).

[6] Ustawa z dn. 9.06.2016 r. o zasadach kształtowania wynagrodzeń osób kierujących niektórymi spółkami (Dz. U. 2020 poz. 1907, ze zm.).

[7] Ustawa z dn. 23.11.2012 r. – Prawo pocztowe (Dz. U. 2022 poz. 896, ze zm.).

III. Niezależność odpowiedzialności kierownika operatora usługi kluczowej

Jak wskazuje się w literaturze (Czaplicki, Gryszczyńska i Szpor, 2019, art. 75, t. 1), kara pieniężna nakładana na kierownika operatora usługi kluczowej jest sankcją wymierzaną niezależnie od kary nakładanej na operatora usługi kluczowej. Istotą deliktu administracyjnego, który może być przypisany kierownikowi operatora usługi kluczowej nie jest natomiast to samo naruszenie obowiązków operatora usługi kluczowej wynikających z ustawy o krajowym systemie cyberbezpieczeństwa, które przypisujemy temu operatorowi, ale odrębne działanie polegające na niedochowaniu przez niego należytej staranności, którą powinien był zachować w celu realizacji obowiązków przypisanych operatorowi usługi kluczowej, z racji pełnionych przez kierownika funkcji zarządczych. Oczywistym jest, że zanim dojdzie do nałożenia tej sankcji, konieczne jest stwierdzenie określonych uchybień w realizacji obowiązków operatora usługi kluczowej, do którego dojść może w szczególności w ramach prowadzenia przez organ właściwy do spraw cyberbezpieczeństwa w ramach monitoringu stosowania przepisów ustawy o krajowym systemie cyberbezpieczeństwa przez operatorów usług kluczowych lub w toku kontroli operatorów usług kluczowych, o których mowa w art. 42 ust. 1 pkt 6 i 8 ustawy o ksc. Ich stwierdzenie skutkuje nałożeniem na operatora kary pieniężnej na podstawie art. 73 ust. 1 pkt 1, 4 i 15 uksc. Czy jednak dla nałożenia kary pieniężnej na kierownika operatora usługi kluczowej konieczne jest uprzednie nałożenie kary pieniężnej na operatora za tego rodzaju naruszenie? Wydaje się, że nie jest to takie oczywiste, ponieważ kierownik operatora nie odpowiada w tym przypadku za to samo naruszenie ustawy o krajowym systemie cyberbezpieczeństwa, co operator. Odpowiedzialność z tytułu naruszenia przez kierownika operatora usługi kluczowej należytej staranności dotyczącej wykonywania obowiązków ustawowych spoczywających na tym operatorze nie jest zatem tożsama z niezależną odpowiedzialnością kierownika podmiotu zbiorowego za delikt popełniony przez podmiot zbiorowy, tak jak ma to miejsce np. w przypadku kary pieniężnej nakładanej na kierownika przedsiębiorstwa energetycznego na podstawie art. 56 ust. 5 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne[8], czy też na kierownika zarządcy i przewoźnika kolejowego na podstawie art. 66 ust. 3 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym[9]. Nie jest to sytuacja analogiczna także do postanowień art. 209 ust. 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[10], gdzie mowa jest o niezależnym karaniu kierującego przedsiębiorstwem telekomunikacyjnym za te same naruszenia, za które karze pieniężnej podlega kierowany przez niego podmiot. W tym przypadku i judykatura[11], i doktryna (Piątek, 2019, s. 1473) stoją na stanowisku, że karę taką nakłada się na kierującego przedsiębiorstwem telekomunikacyjnym jedynie w razie równoległego lub uprzedniego ukarania przedsiębiorcy telekomunikacyjnego. Na gruncie art. 75 ustawy o ksc nie jest to jednak niezależna, równoległa odpowiedzialność kierownika operatora za naruszenie operatora, o którym mowa w art. 73 ustawy o ksc, oparta na koncepcji tzw. winy obiektywnej, ale odpowiedzialność za niezachowanie należytej staranności skutkujące powstaniem określonych naruszeń. Dla nałożenia kary na kierownika operatora usługi kluczowej

[8] Ustawa z dn. 10.04.1997 r. – Prawo energetyczne (Dz. U. 2022 poz. 1385, ze zm.).

[9] Ustawa z dn. 28.03.2003 r. o transporcie kolejowym (Dz. U. 2023 poz. 602, ze zm.).

[10] Ustawa z dn. 16.07.2004 r. – Prawo telekomunikacyjne (Dz. U. 2022 poz. 1648 ze zm.).

[11] Wyr. SN z dn. 23.09.2009 r., III SK 18/09, Legalis nr 212554; wyr. SA w Warszawie z dn. 13.01.2010 r., VI ACa 701/09, Legalis nr 393882.

nie wystarczy zatem jedynie stwierdzenie faktu naruszenia postanowień art. 8 pkt 1, art. 9 ust. 1 pkt 1 oraz art. 15 ust. 1 ustawy o ksc, ale konieczne jest wykazanie, że nie dochował on należytej staranności, w następstwie czego nie wykonano powinności wynikających z tychże przepisów, tj. obowiązku prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem, obowiązku wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz obowiązku przeprowadzenia, nie rzadziej niż raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

Pamiętać jednocześnie trzeba, że w przypadku kar nakładanych na operatora usługi kluczowej na podstawie art. 73 ust. 1 ustawy o ksc, odpowiedzialność ta ma charakter obligatoryjny, ustawodawca posługuje się bowiem sformułowaniem „karze pieniężnej podlega operator usługi kluczowej, który", w przypadku zaś art. 75 ustawy o ksc, mowa jest o możliwości nałożenia kary na kierownika operatora usługi kluczowej, a zatem odpowiedzialność ta ma charakter fakultatywny i mieści się w ramach uznania administracyjnego przysługującego organowi właściwemu do spraw cyberbezpieczeństwa. W razie stwierdzenia naruszeń określonych w art. 73 ust. 1 pkt 1, 4 i 15 ustawy o ksc, do których doprowadził brak należytej staranności kierownika operatora usługi kluczowej i nałożenia kary pieniężnej na tego kierownika zgodnie z art. 75 ustawy o ksc, na operatora usługi kluczowej – nawet jeśli nie uprzednio i nie równolegle – i tak nałożona zostać powinna kara pieniężna. Pamiętać też należy, że o ile w przypadku operatora usługi kluczowej jest to, co do zasady, podmiot zbiorowy, o tyle w przypadku kierownika operatora usługi kluczowej jest to osoba fizyczna, na co wskazuje zarówno ustawowe określenie „kierownik (…), który", jak i sposób określenia wysokości sankcji z odniesieniem do wysokości wynagrodzenia miesięcznego.

IV. Obowiązek zachowania należytej staranności

Jednym ze znamion deliktu administracyjnego, o którym mowa w art. 75 ustawy o ksc, jest niedochowanie należytej staranności przez kierownika operatora usług kluczowych. Materię dochowywania należytej staranności postrzegamy zwykle w pierwszym rzędzie przez pryzmat prawa prywatnego – cywilnego i handlowego. Ustawodawca posługuje się nim w szczególności na gruncie przepisu art. 355 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny[12] (dalej: k.c.), w myśl którego od dłużnika wymaga się zachowania należytej staranności tj. „staranności ogólnie wymaganej w stosunkach danego rodzaju", natomiast w przypadku prowadzenia przez dłużnika działalności gospodarczej, określa się ją z uwzględnieniem zawodowego charakteru tejże działalności. Należyta staranność jest zatem swego rodzaju obiektywnym wzorcem postępowania dłużnika (odnoszącym się do przyjętego sposobu działania, nie zaś jego rezultatów), do którego powinien stosować się dłużnik w toku czynności zmierzających do spełnienia świadczenia, obok zasad współżycia społecznego i zwyczajów, o których mowa w art. 354 k.c. (Załucki, 2023, art. 355, t. I.2.).

Pojęcie „staranności" nieobce jest także ustawie z dnia 15 września 2000 r. – Kodeks spółek handlowych[13] (dalej: k.s.h.). Jak wspomniano powyżej, pod pojęciem „kierownika operatora usługi kluczowej" kryje się w szczególności członek zarządu spółki kapitałowej świadczącej usługę tej

[12] Ustawa z dn. 23.04.1964 r. – Kodeks cywilny (Dz. U. 2022 poz. 1360 ze zm.).

[13] Ustawa z dn.15.09.2000 r. – Kodeks spółek handlowych (Dz. U. 2022 poz. 1467 ze zm.).

kategorii. Warto zatem odnieść się od standardów staranności przypisywanych członkom organów zarządzających w spółkach kapitałowych. W myśl postanowień art. 377[1] § 1 § 1 k.s.h. członek zarządu powinien „przy wykonywaniu swoich obowiązków dołożyć staranności wynikającej z zawodowego charakteru swojej działalności oraz dochować lojalności wobec spółki" (analogicznie do członka rady nadzorczej, art. 387[1] k.s.h.). Co za tym idzie, poziom miernika należytej staranności wymagany od członka zarządu został wyznaczony wyżej aniżeli ten, który określono w art. 355 § 2 k.c. Uwzględnia on bowiem profesjonalny charakter działalności członka organu zarządzającego wymagający w szczególności znajomości specyfiki procesów organizacyjnych i finansowych w zarządzanym podmiocie, zasad gospodarowania jego zasobami, a także, a może przede wszystkim, znajomości przepisów powszechnie obowiązującego prawa i ich wpływu na prowadzoną działalność gospodarczą (Kidyba, 2023, art. 377(1), t. 1). Co więcej, w opinii judykatury nawet „podjęcie się wykonywania obowiązków członka zarządu w sytuacji braku odpowiedniego wykształcenia i wiadomości lub doświadczenia potrzebnego do prowadzenia spraw spółki powinno być kwalifikowane jako naruszenie wymaganej staranności i sumienności"[14]. Wyrazem niedochowania należytej staranności będzie zatem w konsekwencji przyjęcie na siebie obowiązków związanych z pełnieniem funkcji kierownika określonego podmiotu, które nie przystają do posiadanych przez osobę zajmującą dane stanowisko kompetencji zawodowych i zarządczych, w szczególności poziomu znajomości przepisów prawa właściwych dla prowadzenia danej dziedziny działalności gospodarczej.

Z pojęciem „należytej staranności" zetknąć możemy się jednakże i w prawie publicznym. W orzecznictwie sądowoadministracyjnym wydanym na gruncie prawa podatkowego wskazuje się chociażby, że należytej staranności nie zachowuje podatnik, który na skutek swojego niedbalstwa nie posiada wiedzy o istotnym i rzeczywistym stanie faktycznym związanym z naruszeniem prawa[15]. Dołożenia należytej staranności w wyjaśnieniu stronie zasadności podjętego rozstrzygnięcia wymaga się od organu prowadzącego postępowanie administracyjne[16] zgodnie z zasadą przekonywania określoną w art. 11 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[17] (dalej: k.p.a.), w myśl którego „Organy administracji publicznej powinny wyjaśniać stronom zasadność przesłanek, którymi kierują się przy załatwieniu sprawy, aby w ten sposób w miarę możności doprowadzić do wykonania przez strony decyzji bez potrzeby stosowania środków przymusu".

Jak powinien zatem wyglądać model należytej staranności kierownika operatora usługi kluczowej? W orzecznictwie wydanym na gruncie prawa cywilnego wskazuje się, że w dobie szczególnie skomplikowanych stosunków społeczno-gospodarczych i rozwoju techniki, wypracowanie jednego konkretnego modelu przezorności byłoby utrudnione, jeśli nie niemożliwe. Profesjonalizm takiego przedsiębiorcy powinien stanowić sumę dwóch elementów występujących łącznie – fachowości i sumienności[18]. Wykładnia przepisów prawa podatkowego prowadzi NSA do wniosku, że punktem wyjścia dla oceny dochowania należytej staranności przez podatnika są „ogólne kryteria «sumienności kupieckiej», zgodnie z którymi należyta staranność wymagana przy uwzględnieniu

[14] Wyr. SA w Łodzi z dn. 16.04.2014 r., I ACa 1157/13 (Legalis nr 1067291).

[15] Wyr. NSA z dn. 3.03.2023 r., I FSK 2079/18, Legalis nr 2900532.

[16] Wyr. WSA w Poznaniu z dn. 12.02.2020 r., II SA/Po 666/19, LEX nr 2783100.

[17] Ustawa z dn. 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz. U. 2023 poz. 775 ze zm.).

[18] Wyr. SA w Białymstoku z dn. 21.01.2016 r., I ACa 662/15 (LEX nr 1979374).

zawodowego charakteru prowadzonej działalności, uzasadnia zwiększone oczekiwania co do umiejętności, wiedzy, skrupulatności i rzetelności, zapobiegliwości i zdolności przewidywania”[19], przy czym znaczenie może mieć również specyfika branży, w jakiej prowadzi on swoją działalność[20]. Generalnie ujmując, ocena dołożenia należytej staranności uwzględniać powinna w konsekwencji okoliczności konkretnej sytuacji (Michalak, 2016, s. 180–190). Poglądy te zastosowanie mogą mieć w odniesieniu do badania poziomu staranności wymaganej od kierownika operatora usługi kluczowej, mając na względzie szczególny charakter tego rodzaju usług i obowiązków spoczywających na podmiotach je świadczących. Po pierwsze, wymagać należy od niego postępowania zgodnego z regułami fachowej wiedzy, w tym przypadku wymaganej od profesjonalnego menedżera kierującego (współkierującego) podmiotem świadczącym usługi o szczególnej wadze dla należytego funkcjonowania państwa i bezpieczeństwa powszechnego. Wiedza ta powinna obejmować znajomość zarówno profesjonalnych zasad zarządzania zasobami określonej organizacji, jak i uwarunkowań prawnych towarzyszących rodzajowi prowadzonej przez nią działalności. Po drugie, jego aktywność na zajmowanym stanowisku powinna cechować się sumiennością, a zatem skrupulatnym wywiązywaniem się z przyjętych na siebie obowiązków przypisanych określonemu stanowisku kierowniczemu, wykonywaniem ich rzetelnie i ze szczególną dokładnością, a także zdolnością przewidywania następstw podejmowanych działań i konsekwencji poczynionych zaniechań. W świetle analizy poziomu staranności dotyczącej obowiązków kierownika operatora usług kluczowych uwzględnić należy wspomnianą powyżej fachowość i sumienność w odniesieniu do stosowania rozwiązań organizacyjnych i technicznych związanych z przestrzeganiem obowiązków nakładanych na operatora przepisami ustawy o krajowym systemie cyberbezpieczeństwa.

V. Obowiązki operatora usług kluczowych a odpowiedzialność jego kierownika

Karze pieniężnej, o której mowa w art. 75 ustawy o ksc, podlega niezachowanie przez kierownika operatora usługi kluczowej należytej staranności w celu wykonania trzech rodzajów obowiązków spoczywających na tym operatorze. Mieszczące się w ramach należytej staranności profesjonalne i sumienne zarządzanie podmiotem, który świadczy usługę kluczową, służyć ma prawidłowej realizacji tych obowiązków, a jej niedochowanie stanowi przyczynę ich zaniechania lub niewłaściwego (sprzecznego z prawem) wykonywania.

Po pierwsze, powinność zachowania należytej staranności odnosi się do wdrożenia przez operatora usługi kluczowej systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, który zapewnia prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem (art. 8 pkt 1 ustawy o ksc). Zgodnie z motywem 44 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[21], odpowiedzialność za zapewnienie bezpieczeństwa sieci i systemów informatycznych w dużym stopniu spoczywa m.in. na operatorach usług

[19] Wyr. NSA z dn. 25.11.2021 r., I FSK 1574/21, Legalis nr 2663007.

[20] Wyr. NSA z dn. 20.01.2023 r., II FSK 1327/22, Legalis nr 2881314.

[21] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dn. 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE 2016 L 194/1).

kluczowych, a wprowadzenie właściwych wymogów regulacyjnych, określonych właśnie w ustawie o krajowym systemie cyberbezpieczeństwa, służyć ma wsparciu i rozwojowi kultury zarządzania ryzykiem, która obejmuje przeprowadzanie ocen ryzyka i wdrażanie środków bezpieczeństwa odpowiednich dla danego ryzyka. W myśl postanowień art. 14 ust. 1 tejże dyrektywy, państwa członkowskie są obowiązane zapewnić podejmowanie przez operatorów usług kluczowych odpowiednich i proporcjonalnych środków technicznych i organizacyjnych służących zarządzaniu rodzajami ryzyka, na jakie narażone są używane przez nich sieci i systemy informatyczne. Środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych adekwatny do istniejącego ryzyka i uwzględniać najnowszy stan wiedzy. Kierownik operatora usługi kluczowej powinien zatem, zachowując należytą staranność, zadbać o wprowadzenie w zarządzanym przez niego podmiocie stosownych, proporcjonalnych, nowoczesnych, spełniających najlepsze standardy rozwiązań o charakterze technicznym i organizacyjnym, zapewniających prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem we wdrożonym systemie zarządzania bezpieczeństwem, w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej. Co więcej, zadbać powinien w konsekwencji o utrzymywanie tego systemu w należytym stanie (m.in. jego modyfikacji, aktualizacji, dostosowywania do zmian dotyczących sposobu i zasad świadczenia usługi kluczowej itp.). Zaniechanie wdrożenia i monitorowania stanu funkcjonowania – odpowiadającego wymogom ustawowym – systemu zarządzania bezpieczeństwem zapewniającego prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem świadczyć może o niedochowaniu należytej staranności wymaganej od kierownika operatora usługi kluczowej.

Po drugie, wymóg należytej staranności dotyczy wyznaczenia przez operatora usługi kluczowej osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (art. 9 ust. 1 pkt 1 ustawy o ksc)[22]. Należyta staranność kierownika operatora usługi kluczowej wymaga w tym przypadku przede wszystkim wyznaczenia osoby, która z uwagi na posiadane doświadczenie, znajomość zasad i sposobu świadczenia usługi kluczowej u operatora, a także kompetencje merytoryczne, w szczególności znajomość ustawy o krajowym systemie cyberbezpieczeństwa, daje rękojmię sprawnego, efektywnego i zgodnego z prawem kontaktowania się z podmiotami krajowego systemu cyberbezpieczeństwa. Co więcej, z uwagi na wymóg przekazania przez operatora usługi kluczowej do organu właściwego do spraw cyberbezpieczeństwa, właściwego CSIRT MON, CSIRT NASK, CSIRT GOV, a także sektorowego zespołu cyberbezpieczeństwa danych dotyczących tożsamości (imię i nazwisko) oraz danych kontaktowych (numer telefonu, adres poczty elektronicznej) tej osoby, w terminie 14 dni od dnia jej wyznaczenia, jak również informacji o zmianie tych danych – w terminie 14 dni od dnia ich zmiany (art. 9 ust. 2 ustawy o ksc), kierownik operatora usługi kluczowej powinien zadbać również

[22] W skład krajowego systemu cyberbezpieczeństwa wchodzą następujące jednostki: operatorzy usług kluczowych, dostawcy usług cyfrowych; CSIRT MON; CSIRT NASK; CSIRT GOV; sektorowe zespoły cyberbezpieczeństwa; niektóre jednostki sektora finansów publicznych (organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; jednostki samorządu terytorialnego oraz ich związki; związki metropolitalne; jednostki budżetowe; samorządowe zakłady budżetowe; agencje wykonawcze; instytucje gospodarki budżetowej; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; uczelnie publiczne; Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne); instytuty badawcze; Narodowy Bank Polski; Bank Gospodarstwa Krajowego; Urząd Dozoru Technicznego; Polska Agencja Żeglugi Powietrznej; Polskie Centrum Akredytacji; Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej; spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej; podmioty świadczące usługi z zakresu cyberbezpieczeństwa; organy właściwe do spraw cyberbezpieczeństwa; Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa; Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa; Kolegium do Spraw Cyberbezpieczeństwa (art. 4 uksc).

o realizację tego obowiązku, ponieważ zaniechanie jego realizacji skutkuje w rzeczywistości uniemożliwieniem skutecznej komunikacji operatora usługi kluczowej z podmiotami krajowego systemu cyberbezpieczeństwa.

Po trzecie, wymagana należyta staranność kierownika operatora usługi kluczowej odnosi się do obowiązku zapewnienia przeprowadzenia przez tego operatora, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 15 ust. 1 ustawy o ksc). Ustawodawca formułuje w art. 15 uksc wymogi dotyczące częstotliwości i jakości tego rodzaju badania. W zakresie terminu jego przeprowadzenia spoczywa na operatorze wymóg jego powtarzania co najmniej co 2 lata. Rękojmię zapewnienia właściwego standardu merytorycznego stanowić ma wykonanie audytu przez podmioty wykazujące się przymiotami określonymi przez ustawodawcę. W zależności od rozmiarów działalności prowadzonej przez operatora usługi kluczowej naruszeniem należytej staranności będzie zatem niepodjęcie środków wprowadzających określone mechanizmy (sformalizowane procesy, procedury) zapewniające regularne i profesjonalne (przez podmioty spełniające wymagania ustawowe) przeprowadzenie audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, jak również – jeśli przyjęto tego rodzaju rozwiązanie – okresowe zlecanie/zarządzanie przeprowadzenia audytu wymaganego postanowieniami ustawy o krajowym systemie cyberbezpieczeństwa. Pamiętać należy, że zgodnie z art. 15 ust. 7 ustawy o ksc, operator usługi kluczowej zobowiązany jest przekazać kopię sprawozdania z przeprowadzonego audytu na uzasadniony wniosek organu właściwego do spraw cyberbezpieczeństwa (jak również dyrektora Rządowego Centrum Bezpieczeństwa lub Szefa Agencji Bezpieczeństwa Wewnętrznego). Fakt niewywiązania się z obowiązków spoczywających na operatorze usług kluczowych, a w konsekwencji fakt niedołożenia należytej staranności przez kierownika, w odniesieniu do powinności przeprowadzenia audytu, może zostać stwierdzony przez organ właściwy do spraw cyberbezpieczeństwa w sytuacji niedostarczenia ww. kopii.

VI. Wymiar i przeznaczenie kary pieniężnej

Wymiar kary pieniężnej określany jest przez ustawodawcę na gruncie powszechnie obowiązującego prawa w sposób rozmaity – zwykle kwotowo lub procentowo, w postaci sankcji oznaczonej bezwzględnie lub względnie. W przypadku ustawy o krajowym systemie cyberbezpieczeństwa kara pieniężna nakładana na kierownika operatora usługi kluczowej nie może przekroczyć równowartości 200% jego miesięcznego wynagrodzenia (art. 75 ustawy o ksc *in fine*). Ustawa nie określa w sposób dokładny, o jak rozumiane wynagrodzenie miesięczne tutaj chodzi. Niemniej wydaje się, że można przyjąć chociażby za przywołaną już powyżej ustawą – Prawo telekomunikacyjne, gdzie w myśl postanowień art. 209 ust. 2 tego aktu normatywnego, Prezes Urzędu Komunikacji Elektronicznej może nałożyć karę pieniężną na kierującego przedsiębiorstwem telekomunikacyjnym „w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy”, iż mowa jest tutaj o wynagrodzeniu miesięcznym naliczanym w taki właśnie sposób. W literaturze podnosi się natomiast, że wysokość kary pieniężnej powinno obliczać się wg kwoty wynagrodzenia netto (Besiekierska, 2019, art. 75, t. 3). Co więcej uznać należy, że przez pojęcie wynagrodzenia miesięcznego jako podstawy naliczenia kary pieniężnej

rozumie się jedynie wynagrodzenie miesięczne osiągane z tytułu pełnienia funkcji kierownika operatora usługi kluczowej, a nie wynagrodzenie miesięczne osiągane ogółem przez sprawcę analizowanego deliktu administracyjnego, również z tytułu innych aktywności zawodowych czy źródeł przychodu.

Określając wysokość kary, organ właściwy do spraw cyberbezpieczeństwa kieruje się, wobec braku ustawowych dyrektyw wymiaru tej sankcji w ustawie o krajowym systemie cyberbezpieczeństwa, wytycznymi wskazanymi w art. 189d k.p.a., do których zaliczono: „1) wagę i okoliczności naruszenia prawa, w szczególności potrzebę ochrony życia lub zdrowia, ochrony mienia w znacznych rozmiarach lub ochrony ważnego interesu publicznego lub wyjątkowo ważnego interesu strony oraz czas trwania tego naruszenia; 2) częstotliwość niedopełniania w przeszłości obowiązku albo naruszania zakazu tego samego rodzaju co niedopełnienie obowiązku albo naruszenie zakazu, w następstwie którego ma być nałożona kara; 3) uprzednie ukaranie za to samo zachowanie za przestępstwo, przestępstwo skarbowe, wykroczenie lub wykroczenie skarbowe; 4) stopień przyczynienia się strony, na którą jest nakładana administracyjna kara pieniężna, do powstania naruszenia prawa; 5) działania podjęte przez stronę dobrowolnie w celu uniknięcia skutków naruszenia prawa; 6) wysokość korzyści, którą strona osiągnęła, lub straty, której uniknęła; 7) w przypadku osoby fizycznej – warunki osobiste strony, na którą administracyjna kara pieniężna jest nakładana”. Część spośród tych wyznaczników w sposób jednoznaczny związana jest z materią staranności działania kierownika operatora usługi kluczowej. Mowa tutaj w szczególności o elementach odnoszących się do dotychczasowego zachowania osoby podlegającej karze pieniężnej, np. częstotliwości niedopełniania w przeszłości spoczywającego na niej obowiązku (zachowania należytej staranności) czy też stopniu przyczynienia się sprawcy deliktu administracyjnego do powstania naruszenia prawa (poziomie niedopełnienia obowiązku dochowania należytej staranności).

Nadmienić wreszcie trzeba, że ustawodawca nie wskazuje przeznaczenia środków finansowych pochodzących z kary pieniężnej nakładanej na kierownika operatora usług kluczowych, jak ma to miejsce w odniesieniu do wpływów z tytułu kar pieniężnych, o których mowa w art. 73 ustawy o ksc, które stanowią przychód Funduszu Cyberbezpieczeństwa[23] (art. 74 ust. 2 ustawy o ksc). Nie określa w szczególności, że środki te stanowią dochód budżetu państwa, jak czyni to np. w art. 130 ustawy – Prawo pocztowe lub art. 104 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[24]. Niemniej, skoro przepis art. 111 ust. 1 pkt 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[25] zalicza do dochodów budżetu państwa w szczególności „grzywny, mandaty i inne kary pieniężne, o ile odrębne ustawy nie stanowią inaczej”, to wobec braku stosownego unormowania w tej materii na gruncie ustawy o krajowym systemie cyberbezpieczeństwa przyjąć należy, że kara pieniężna nakładana na operatora usługi kluczowej zgodnie z art. 75 ustawy o ksc stanowi dochód budżetu państwa.

[23] Zgodnie z postanowieniami art. 2 ustawy z dn. 2.02.2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. 2023 poz. 667), Fundusz Cyberbezpieczeństwa jest państwowym funduszem celowym, którego dysponentem jest minister właściwy do spraw informatyzacji, a jego celem jest wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami.

[24] Ustawa z dn. 10.05.2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781).

[25] Ustawa z dn. 27.08.2009 r. o finansach publicznych (Dz. U. 2023 poz. 1270 ze zm.).

VII. Decyzja w sprawie nałożenia kary pieniężnej

Karę pieniężną na kierownika operatora usługi kluczowej, podobnie jak na samego operatora, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa (Banasiński i Rojszczyk, 2020, rozdz. 1, pkt 2). Organami właściwymi do spraw cyberbezpieczeństwa są:

– minister właściwy do spraw energii – dla sektora energii;
– minister właściwy do spraw transportu – dla sektora transportu z wyłączeniem podsektora transportu wodnego;
– minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej – dla podsektora transportu wodnego;
– Komisja Nadzoru Finansowego – dla sektora bankowego i infrastruktury rynków finansowych;
– minister właściwy do spraw gospodarki wodnej – dla sektora zaopatrzenia w wodę pitną i jej dystrybucji;
– Minister Obrony Narodowej – dla sektora ochrony zdrowia, sektora infrastruktury cyfrowej oraz dla dostawców usług cyfrowych obejmujących podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej oraz przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych obejmujące: wykonywanie produkcji, napraw lub świadczenie usług na rzecz Sił Zbrojnych w warunkach zagrożenia bezpieczeństwa państwa lub w czasie wojny; utrzymywanie w czasie pokoju mocy produkcyjnych, naprawczych lub usługowych niezbędnych do realizacji powyższych zadań; militaryzację; ochronę obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa; inne zadania realizowane na rzecz Sił Zbrojnych i wojsk sojuszniczych;
– minister właściwy do spraw informatyzacji – dla sektora infrastruktury cyfrowej i dla dostawców usług cyfrowych z wyłączeniem ww. podmiotów podległych Ministrowi Obrony Narodowej i przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych;
– minister właściwy do spraw zdrowia – dla sektora ochrony zdrowia z wyłączeniem ww. podmiotów podległych Ministrowi Obrony Narodowej i przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych (art. 41 ustawy o ksc).

Przepisy rozdziału 14 pt. „Przepisy o karach pieniężnych" nie regulują takich kwestii, jak przesłanki wymiaru administracyjnej kary pieniężnej, zasady odstąpienia od jej nałożenia, przedawnienia jej nakładania i egzekucji, odsetek od zaległej kary pieniężnej czy też udzielania ulg w jej wykonaniu, dlatego też do deliktu tego zastosowanie mają w pełni przepisy działu IVa k.p.a. pt. „Administracyjne kary pieniężne". W konsekwencji, w myśl postanowień art. 189f § 1 k.p.a., organ właściwy do spraw cyberbezpieczeństwa obowiązany będzie, w drodze decyzji, odstąpić od nałożenia kary pieniężnej i poprzestać na pouczeniu kierownika operatora usługi kluczowej, jeśli waga naruszenia prawa, a zatem stopień niedołożenia należytej staranności okaże się znikomy, strona zaś zaprzestała naruszania prawa, czyli podjęła kroki zmierzające do realizacji przez kierowanego przez nią operatora usług kluczowych obowiązków określonych w art. 8 pkt 1, art. 9 ust. 1 pkt 1 oraz art. 15 ust. 1 ustawy o ksc.

VIII. Uwagi końcowe

Przepisy ustawy o krajowym systemie cyberbezpieczeństwa regulują materię odpowiedzialności kierownika operatora usługi kluczowej w sposób fragmentaryczny, nawet w porównaniu z przepisami dotyczącymi zasad nakładania kar pieniężnych na operatora usługi kluczowej czy operatora usługi cyfrowej. Nie określa w szczególności takich kwestii, jak dyrektywy wymiaru kary, zasady odstąpienia od jej nałożenia, przeznaczenie środków uzyskiwanych z tytułu kar pieniężnych, sposobu obliczania wynagrodzenia stanowiącego podstawę wymiaru kary pieniężnej. O niektórych spośród nich wspomniano już powyżej. Warto pokusić się jednakże o wskazanie pewnych obszarów, gdzie zasadne mogłoby okazać się rozważenie pewnych zmian legislacyjnych. Na wstępie wskazać należy chociażby potrzebę określenia przeznaczenia środków pochodzących z kary pieniężnej nałożonej na podstawie art. 75 ustawy o ksc, które – analogiczne do przypadku sankcji nakładanych na podstawie art. 73 ustawy o ksc na operatora usługi kluczowej i operatora usługi cyfrowej – zasilać mogłyby, jak się wydaje z powodów uzasadnionych regulowaną materią ustawową, Fundusz Cyberbezpieczeństwa. Zastanawia również dobór niewykonanych obowiązków operatora usługi kluczowej, stanowiących konsekwencję niedochowania należytej staranności przez jego kierownika skutkującą poniesieniem przez niego odpowiedzialności karnoadministracyjnej. W katalogu naruszeń stypizowanych w art. 73 ustawy o ksc znajduje się chociażby delikt administracyjny polegający na zaniechaniu powołania przez operatora usługi kluczowej wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcia umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (art. 73 ust. 1 pkt 10 ustawy o ksc). Z pewnością realizacja tego rodzaju obowiązków uzależniona jest od należytego pełnienia swoich obowiązków przez kierownika tego operatora. Czy nie warto byłoby się zastanowić także nad zasadnością objęcia tego rodzaju „współodpowiedzialnością" chociażby stanu faktycznego, w którym organ właściwy do spraw cyberbezpieczeństwa stwierdza w wyniku kontroli, że operator usługi kluczowej uporczywie narusza przepisy ustawy o krajowym systemie cyberbezpieczeństwa, co powoduje bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, a także zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych. Ocena szkodliwości społecznej tego deliktu dokonana przez ustawodawcę i uznanie go za szkodliwy społecznie w stopniu wyższym niż delikty wskazane w art. 73 ust. 1 ustawy o ksc skutkuje przecież tym, że podlega on sankcji bardziej dolegliwej – karze pieniężnej w wysokości do 1 000 000 zł (art. 73 ust. 5 ustawy o ksc). Uporczywe, a zatem powtarzające się i występujące relatywnie długo, naruszenie świadczy natomiast o braku należytej staranności kierownika określonego podmiotu w zapewnieniu stanu przestrzegania prawa przez podległy mu pomiot.

Bibliografia

Banasiński, C. i Rojszczyk, M. (red.). (2020). *Cyberbezpieczeństwo*. Wolters Kluwer Polska.

Besiekierska, A. (red.). (2019). *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Wydawnictwo C.H. Beck.

Crafoord, C. i Nykvist, O. (2021). Företagens minimirättigheter enligt Europakonventionen vid påförande av administrativa sanktionsavgifter. *Svensk Juristtidning*, (10).

Czaplicki, K., Gryszczyńska, A. i Szpor, G. (red.). (2019). *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Wolters Kluwer Polska.

Kidyba, A. (2023). *Komentarz aktualizowany do art. 301–633 Kodeksu spółek handlowych*. Wolters Kluwer/LEX/el.

Kitler, W., Taczkowska-Olszewska, J. i Radoniewicz, F. (red.). (2019). *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Wydawnictwo C.H. Beck.

Michalak, M. (2016). Należyta staranność i dobra wiara w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej oraz polskich sądów administracyjnych. *Studia Iuridica Toruniensia*, *XIX*.

Piątek, S. (2019). *Prawo telekomunikacyjne. Komentarz*. Wydawnictwo C.H. Beck.

Sobol, E. (red.). (2006). *Nowy słownik języka polskiego PWN*. PWN.

Załucki, M. (red.). (2023). *Kodeks cywilny. Komentarz*. Wydawnictwo C.H. Beck.