Paweł Wajda*

Cyberbezpieczeństwo – sektorowe aspekty regulacyjne

Spis treści

Streszczenie

Niniejszy artykuł poświęcony jest analizie regulacyjnej postanowień ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Celem artykułu jest wykazanie – po pierwsze, że w przypadku powołanej ustawy mamy do czynienia z tzw. regulacją sektorową, która nakierowana jest na wypracowanie innych celów niżeli zapewnienie konkurencji w obrębie rynku (jak ma to miejsce w przypadku klasycznej regulacji gospodarczej). Po drugie, wykazanie, że w przypadku celu, jakim jest cyberbezpieczeństwo, mamy do czynienia z wypracowywaniem tego celu w sposób wyłącznie pośredni. Po trzecie wreszcie, celem niniejszego opracowania jest przedstawienie instytucji służących zapewnieniu cyberbezpieczeństwa, tj. scharakteryzowanie i ocena obowiązków operatorów usług kluczowych i dostawców usług cyfrowych.

Słowa kluczowe: teoria regulacji; regulacja sektorowa; cyberbezpieczeństwo; operator usług kluczowych; dostawca usług cyfrowych.

JEL: K24

I. Wprowadzenie

W mojej ocenie pewnym fenomenem współczesnego, czy też aktualnego (bo w istocie tendencja ta nabrała szczególnego nasilenia dopiero po ostatnim globalnym kryzysie finansowym), prawa publicznego gospodarczego jest tendencja do obejmowania przez unijnego i – niejako w ślad za nim – krajowego prawodawcę coraz większego obszaru systemu gospodarczego. Z powodzeniem można wskazać, że w ostatniej dekadzie istotnemu zwiększeniu uległa liczba regulacji gospodarczych, a jednocześnie proporcjonalnemu zmniejszeniu uległ ten obszar systemu gospodarczego, w ramach którego można mówić o niemal pełnej swobodzie działalności gospodarczej. W piśmiennictwie trafnie przy tym, bazując na powyższym fenomenie, podnosi się,

* Profesor doktor habilitowany, Katedra Prawa i Postępowania Administracyjnego, Wydział Prawa i Administracji, Uniwersytet Warszawski; adwokat, *of counsel* w kancelarii Baker & McKenzie; e-mail: p.wajda@wpia.uw.edu.pl; https://orcid.org/0000-0003-4423-8881.

że sama regulacja powinna być rozumiana możliwie szeroko jako całość oddziaływania państwa (władzy publicznej) na zachowania uczestników rynku (por. szerzej: Długosz, 2013, s. 698), gdzie tego oddziaływania jest coraz więcej i odbywa się ono w coraz większym wymiarze.

Aktualnie mamy do czynienia wręcz ze swoistą rewolucją regulacyjną, której wyróżnikiem jest po pierwsze obejmowanie regulacją coraz to nowych obszarów systemu gospodarczego (czego czytelnym przykładem są podejmowane próby uregulowania nowych technologii, tworzonych w sposób wolny i spontaniczny; przy czym, niejednokrotnie, jako odpowiedź rynku na coraz bardziej nasilone regulacje tradycyjnych rynków, czego czytelnym przykładem są tzw. *fin-tech'y*), po drugie zaś pewna technicyzacja regulacji i obejmowanie regulacją coraz bardziej technicznych obszarów związanych z funkcjonowaniem szeroko rozumianego obrotu gospodarczego. W obszarze regulacji gospodarczej mamy aktualnie do czynienia ze zjawiskiem swoistej technicyzacji, gdzie regulacja ta staje się coraz bardziej oderwana od klasycznego brzmienia przepisów prawa, które to przepisy mają być powszechnie zrozumiałe, ponadto regulacja ta obejmuje obszary coraz bardziej techniczne i bliższe naukom politechnicznym niżeli uniwersyteckim.

Wskazana technicyzacja regulacji gospodarczych jest wynikiem technicyzacji życia społecznego i gospodarczego, które to w coraz większym stopniu odbywa się z wykorzystaniem elektronicznych środków komunikacji na odległość, w tym przede wszystkim z wykorzystaniem transmisji danych w ramach sieci Internet. Historia gospodarcza podpowiada przy tym, że zawsze wraz z rozwojem nowych technologii pojawiały się zjawiska patologiczne, które wymagały odpowiedniej interwencji prawodawcy nakierowanej na mitygowanie ryzyka prawnego związanego z rozwojem nowych technologii.

W powyższym kontekście warto za K. Strzyczkowskim podnieść, że w tradycyjnym ujęciu przyjmuje się, że regulacja gospodarcza jest jedną z zasadniczych funkcji ingerencji władzy publicznej i państwa w gospodarkę rynkową, której to zasadniczym celem jest zastąpienie mechanizmów rynkowych i konkurencji w tych obszarach działalności gospodarczej, w których mechanizmy te naturalnie nie funkcjonują (por. szerzej: Strzyczkowski, 2010, s. 160). Oczywistym jest bowiem, że w praktyce obrotu gospodarczego niejednokrotnie mamy do czynienia z sytuacją, w której to pewien obszar, w sposób niejako naturalny niezwiązany z regulacją normatywną, pozostaje początkowo totalnie poza obszarem zainteresowania prawodawcy i organów administracji publicznej i w miarę pojawiania się w tym obszarze zachowań o walorze patologicznym (jak np. koncentrowania działalności przestępczej), zostaje poddany regulacji. W istocie zatem można powiedzieć, że w niejako *klasycznej* nauce prawa publicznego gospodarczego przyjmuje się, że regulacja gospodarcza nakierowana jest na wyeliminowanie niepożądanych zachowań i wsparcie mechanizmu rynkowego (zob. Hoff, 2008, s. 22).

W powyższym kontekście należy dodatkowo wskazać, że aktualnie regulacje gospodarcze realizują zdecydowanie więcej celów regulacyjnych niżeli prokonkurencyjne oddziaływanie na rynek. Stąd też niejednokrotnie w *nowym* piśmiennictwie odróżnia się regulację prokonkurencyjną (tj. nakierowaną właśnie na zapewnienie właściwego działania mechanizmu konkurencji) od regulacji sektorowej (tj. nakierowanej na realizację bardziej rozbudowanych, specyficznych dla danego sektora gospodarki, celów jak np. zapewnienie bezpieczeństwa transportu) (zob. Skoczny, 2013, s. 1359–1362).

W mojej ocenie bardzo dobrym przykładem tego ostatniego zjawiska, gdzie regulacji został poddany obszar, który w swoim pierwotnym założeniu miał być wolny od regulacji i gdzie regulacja

nakierowana jest na realizację innych celów niżeli zapewnienie prokonkurencyjnego działania rynku, są postanowienia ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU 2018, poz. 1560, ze zm.; dalej: uksc), tj. postanowienia systemowej regulacji w obszarze zapewnienia bezpieczeństwa cyfrowego, czyli niezakłóconego świadczenia usług kluczowych i usług cyfrowych, co ma odbyć się poprzez wypracowanie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia usług kluczowych i cyfrowych, a także poprzez zapewnienie odpowiedniej obsługi incydentów bezpieczeństwa.

Z powodzeniem mogę wskazać, że aktualnie – w ramach rozwiniętych społeczeństw i systemów gospodarczych – wręcz niemożliwym do wyobrażenia jest efektywne funkcjonowanie obrotu społecznego i gospodarczego bez wykorzystania sieci Internet i innych sieci umożliwiających przesyłanie danych z wykorzystaniem elektronicznych środków komunikacji na odległość. Sieci te związane są ze specyficznymi rodzajami ryzyka, które to muszą być odpowiednio adresowane przez prawodawcę w treści aktów normatywnych. Przykładowo – odwołując się doświadczeń płynących z sektora finansowego, który związany jest ze świadczeniem usług kluczowych, o których jest mowa w uksc, należy wskazać, że jeszcze dwie dekady temu wykorzystanie bankowości elektronicznej w Polsce było tak niewielkie, że ryzyko związane z tzw. atakami phishingowymi na klientów bankowości elektronicznej dotykało siłą rzeczy bardzo niewielką liczbę adresatów, co czyniło te ataki często mało atrakcyjnymi dla przestępców. Swoje działania przy atakach phishingowych kierują oni bowiem do możliwie szerokiego grona użytkowników bankowości elektronicznej, by maksymalizować rezultaty ekonomiczne takiej nieprawidłowej i nielegalnej działalności.

Natomiast dzisiaj mamy do czynienia z sytuacją, w której to właśnie przestępstwa internetowe wymierzone niejako w klientów instytucji finansowych są niezwykle atrakcyjne z punktu widzenia działalności prowadzonej przez zorganizowane grupy przestępcze. Zjawisko to jest niewątpliwie istotnym wyzwaniem dla prawodawcy, który zobligowany jest podejmować zintensyfikowane działania nakierowane na ograniczenie negatywnej ekspozycji związanej z tym ryzykiem, tak by uniknąć sytuacji, w której bankowość elektroniczna nie będzie w ogólności podlegać rozwojowi z uwagi na brak zaufania do niej pośród jej użytkowników. Tym samym mamy do czynienia z sytuacją, gdy to oddziaływanie na konkurencyjność rynku schodzi niejako na dalszy plan, a celem regulacji jest zapewnienie bezpieczeństwa (w tym wypadku cyberbezpieczeństwa) działania rynku. W tym miejscu warto dodatkowo zasygnalizować, że analizowana ustawa jest specyficzna jeszcze z jednego punktu widzenia. Mamy tutaj do czynienia z tzw. pośrednim oddziaływaniem, tj. prawodawca poprzez oddziaływanie na makropoziomie zamierza zapewnić cyberbezpieczeństwo na poziomie mikro. Jest to pewne *novum*, albowiem zwyczajowo przy regulacji gospodarczej prawnicy są niejako przyzwyczajeni właśnie do oddziaływania na poziomie mikro.

II. Cyberbezpieczeństwo – uwagi ogólne

Powołana ustawa nie jest pomysłem krajowym, ponieważ w zakresie swojej regulacji wdraża do polskiego systemu normatywnego Dyrektywę 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 (Dz. Urz. UE L 194 z 19.07.2016, s. 1).

Mając powyższe na uwadze, należy wskazać, że zgodnie z zasadami tzw. prounijnej wykładni przepisów prawa krajowego[1] konieczne jest odwołanie się do odpowiednich postanowień tej dyrektywy, gdy dokonuje się wykładni przepisów uksc. Należy więc w pierwszej kolejności wskazać że zgodnie z motywami 1–3 dyrektywy prawodawca unijny podkreśla, że sieci oraz systemy i usługi informatyczne odgrywają ważną rolę w społeczeństwie. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i społecznej, w szczególności dla funkcjonowania rynku wewnętrznego. Skala, częstotliwość oraz wpływ incydentów w zakresie bezpieczeństwa stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Systemy te mogą się również stać obiektem umyślnych szkodliwych działań, mających na celu uszkodzenie lub przerwanie ich działania. Tego typu incydenty mogą utrudniać prowadzenie działalności gospodarczej, powodować znaczne straty finansowe, podważać zaufanie użytkowników oraz powodować poważne straty w gospodarce Unii Europejskiej. Sieci i systemy informatyczne, a przede wszystkim Internet znacznie ułatwiają transgraniczny przepływ towarów, usług i osób. Ze względu na ponadnarodowy charakter tych systemów, ich znaczne zakłócenia – niezależnie czy umyślne, czy nieumyślne oraz od tego, gdzie występują – mogą mieć wpływ zarówno na poszczególne państwa członkowskie, jak i na całą na Unię. Bezpieczeństwo sieci i systemów informatycznych ma zatem zasadnicze znaczenie dla sprawnego funkcjonowania rynku wewnętrznego. Bezpieczeństwo to ma zatem, koncentrując dalsze rozważania na wpływie rozwiązań normatywnych dotyczących cyberbezpieczeństwa na użytkowników usług kluczowych i usług cyfrowych, krytyczne znaczenie dla wszystkich podmiotów prawa w ramach Unii Europejskiej, które to podmioty są częstokroć końcowymi beneficjentami usług kluczowych oraz usług cyfrowych.

Ratio regulacji tak z Ddyrektywy, jak i z uksc jest więc ochrona użytkowników usług kluczowych oraz usług cyfrowych przed negatywną ekspozycją tych użytkowników na ryzyka specyficzne związane z brakiem odpowiedniego poziomu cyberbezpieczeństwa. Prawodawca, określając standard świadczenia usług kluczowych i usług cyfrowych w zakresie cyberbezpieczeństwa, który to standard ma być stosowany przez operatorów usług kluczowych oraz przez dostawców usług cyfrowych, ma za zadanie chronić przede wszystkim końcowych beneficjentów tych usług.

W tym miejscu konieczne jest podkreślenie, że jakkolwiek końcowi użytkownicy usług kluczowych lub cyfrowych nie są z całą pewnością bezpośrednim adresatem postanowień czy to powołanej wyżej dyrektywy, czy też uksc (w tym kontekście należy bowiem zauważyć, że w zakresie podmiotowym zastosowania tej ustawy, który to zakres został określony w art. 4 uksc użytkownicy ci nie zostali w ogólności wskazani, co jest bezpośrednim potwierdzeniem tego, że intencją prawodawcy nie było to, by postanowienia uksc znajdowały bezpośrednie zastosowanie do beneficjentów usług kluczowych lub usług cyfrowych), to ustawa ta ma szczególnie doniosłe znaczenie dla użytkowników usług kluczowych lub cyfrowych.

Ustawa stanowi, co było sygnalizowane, bowiem *sui generis* gwarancję, że usługi kluczowe i usługi cyfrowe będą realizowane przez ich odpowiednio operatorów i dostawców w sposób cyberbezpieczny, a tym samym w sposób zapewniający użytkownikom tych usług możliwość

[1] Por. szerzej: wyr. TS z 10.04.1984 r. w sprawie 14/83, *von Colson i Kamann v. Nadrenia Północna-Westfalia*, ECR 1984, s. 1891, pkt 26; z 8.10.1987 r. w sprawie 80/86 *Kolpnighuis Nijmegen*, ECR 1987, s. 3969, pkt 12; z 13.11.1990 r., w sprawie C-106/89, *Marleasing*, ECR 1990, s. I-4135, pkt 8; z 9.03.2004 r., w połączonych sprawach: od C-397/01 do C-403/01, *Pfeiffer*, Zb. Orz. 2004, s. I-8835, pkt 113.

bezpiecznego i niezakłóconego incydentami z nich korzystania. W rezultacie z powodzeniem można przyjąć, że to właśnie końcowi użytkownicy usług kluczowych i cyfrowych są pośrednim adresatem postanowień uksc, a korelatem obowiązków publicznoprawnych spoczywających na podmiotach wymienionych w art. 4 uksc jest uprawnienie użytkowników usług kluczowych i cyfrowych do bezpiecznego i niezakłóconego incydentami korzystania z tych usług. Należy przy tym wyraźnie wskazać, że prawodawca, chroniąc w końcowym rozrachunku przede wszystkim interesy końcowych użytkowników, chroni jednocześnie interesy operatorów usług kluczowych i dostawców usług cyfrowych. W sytuacji bowiem gdyby usługi te nie charakteryzowały się odpowiednim poziomem cyberbezpieczeństwa, usługobiorcy nie korzystaliby z tych usług w ogólności lub korzystali tylko w koniecznym zakresie, co siłą rzeczy miałoby negatywne przełożenie na wyniki finansowe wypracowywane w ramach tej działalności przez odpowiednio operatorów usług kluczowych oraz dostawców usług cyfrowych. W sytuacji bowiem, gdyby końcowi użytkownicy niejako nie wierzyli w to, że usługi kluczowe i usługi cyfrowe charakteryzują się odpowiednim poziomem cyberbezpieczeństwa, to oczywistym jest, że ci użytkownicy nie korzystaliby z tych usług w takim stopniu, jak czynią to w sytuacji pozytywnej wiary w cyberbezpieczeństwo tych usług.

Mamy zatem do czynienia z klasycznym rozwiązaniem, w ramach którego obowiązek podmiotu publicznego (jak np. wymienione w art. 4 uksc organy administracji publicznej), czy też podmiotu *quasi*-publicznego (jak np. operator usług kluczowych czy dostawca usług cyfrowych), jest skorelowany z uprawnieniem użytkownika usług kluczowych i cyfrowych do bezpiecznego i niezakłóconego incydentami korzystania z tych usług. Obowiązek publicznoprawny z uksc jest zatem ściśle połączony z uprawnieniem użytkownika usług kluczowych i cyfrowych, tak w obszarze możliwości korzystania z tych usług w ogólności, jak i w obszarze bezpiecznego i niezakłóconego incydentami korzystania. Rozwiązanie to jest z powodzeniem wykorzystywane w obrębie wielu rynków regulowanych; przykładowo warto wskazać, że rozwiązanie to jest jednym z zasadniczych rozwiązań, które zostało wprowadzone do systematyki ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi w związku z implementacją dyrektywy MiFID II. W rezultacie jako wręcz pewien standard rynkowy można postrzegać, że beneficjentem obowiązku nałożonego na podmiot profesjonalny jest użytkownik usługi świadczonej przez ten podmiot profesjonalny. Tym samym za uprawnione należy uznać stanowisko, że w przypadku regulacji cyberbezpieczeństwa mamy do czynienia z tzw. regulacją sektorową, a nie regulacją prokonkurencyjną. Zasadniczym celem tej regulacji nie jest bowiem zapewnienie konkurencji, a realizacja celu sprowadzającego się do zapewnienia właśnie cyberbezpieczeństwa. W konsekwencji z pełnym przekonaniem można wskazać, że uksc jest regulacją specyficzną w ramach całego katalogu regulacji gospodarczych, co jest predestynowane przez *ratio legis* przepisów uksc.

Powyższe założenie wyznaczy jednocześnie strukturę niniejszego opracowania, w ramach którego autor podda analizie obowiązki podmiotów profesjonalnych, jak operatorzy usług kluczowych oraz dostawcy usług cyfrowych z punktu widzenia faktycznego wpływu tych obowiązków na zapewnienie odpowiedniego – prawem określonego – poziomu bezpieczeństwa dla końcowych beneficjentów tych usług.

W tym miejscu celowe jest podkreślenie, że znaczenie tej regulacji dla użytkowników usług kluczowych lub cyfrowych jest tym większe, że aktualnie mamy do czynienia – co było już sygnalizowane – ze swoistą cyfryzacją życia społecznego i gospodarczego. Zjawisko to jest nasilone

już na takim poziomie intensywności, że mogę z powodzeniem zaryzykować postawienie tezy, że w rozwiniętych społeczeństwach trudno byłoby sobie wyobrazić aktualnie życie bez dostępu do usług cyfrowych, czy też takie swoiste wykluczenie cyfrowe tych podmiotów. Z każdym rokiem coraz większy obszar życia społecznego i gospodarczego jest bowiem nieodłącznie powiązany z usługami cyfrowymi, co z jednej strony tworzy istotne szanse szczególnie w obszarze dalszego dynamicznego rozwoju tych usług i możliwości prowadzenia rentownej działalności usługowej, z drugiej natomiast nieodłącznie powiązane jest z ryzykiem nieprawidłowego funkcjonowania tych usług. Ryzyko to związane jest tak z samymi błędami i niedoskonałościami w zakresie świadczenia tych usług, jak i – co ma swój zdecydowanie bardziej doniosły społecznie i gospodarczo wymiar – z działaniami o charakterze przestępczym, tj. z działaniami które objęte są dyspozycjami odpowiednich przepisów zaliczanych do gałęzi prawa karnego. W tym ostatnim kontekście celowe jest przypomnienie, że coraz częściej jesteśmy informowani przez media o tym, że w ramach świadczenia usług cyfrowych podejmowane są przez przestępców działania objęte dyspozycjami odpowiednich przepisów prawa karnego (np. przestępstwo kradzieży, przestępstwo oszustwa, etc.), które to działania, co do zasady, mają na celu na osiągnięcie nielegalnego zysku kosztem użytkowników usług cyfrowych. Działanie te mają przy tym to do siebie, że w przypadku popełnienia takiego przestępstwa ma ono nieograniczony krąg ofiar. Pewne osoby są nim bowiem dotknięte bezpośrednio (i stanowią jego bezpośrednią ofiarę), inne zaś (inni użytkownicy usług kluczowych lub usług cyfrowych) – pośrednio. Każdy bowiem taki czyn przestępczy skutkuje spadkiem poziomu zaufania do cyfrowych usług i kryzysem w zakresie poczucia się cyberbezpiecznym. W konsekwencji z powodzeniem można wskazać, że właściwa i pełna realizacja przez podmioty wymienione w art. 4 uksc ich obowiązków publicznoprawnych jest działaniem, które leży w żywotnym interesie społecznym, wszystkich użytkowników usług kluczowych i cyfrowych oraz całego systemu gospodarczego.

Jak zostało to już wskazane, użytkownicy usług kluczowych lub usług cyfrowych nie są bezpośrednimi adresatami norm uksc. Ustawa ta nie znajduje w rezultacie w ogólności bezpośredniego zastosowania do działalności tych użytkowników, nie nakłada też na nich jakichkolwiek obowiązków związanych z cyberbezpieczeństwem, w rezultacie nie można w jakimkolwiek przypadku mówić o bezpośrednim związku pomiędzy postanowieniami uksc a cyberbezpieczeństwem. Można natomiast z powodzeniem mówić – co będzie przedmiotem poszerzonych analiz w dalszej części niniejszego opracowania – o związku pośrednim; jak zostało to bowiem zasygnalizowane, prawidłowa realizacja przez operatorów usług kluczowych i przez dostawców usług cyfrowych ich obowiązków w obszarze cyberbezpieczeństwa przekłada się w końcowym rozrachunku na zapewnienie odpowiedniego poziomu ochrony w obszarze cyberbezpieczeństwa.

III. Obowiązki operatorów usług kluczowych

Ta ostatnia konstatacja wyznacza jednocześnie strukturę niniejszego opracowania. Przedmiotem analiz będzie bowiem ocena obowiązków odpowiednio operatorów usług kluczowych oraz dostawców usług cyfrowych w obszarze cyberbezpieczeństwa, która to będzie dokonywana z punktu widzenia czy rozwiązania te przekładają się na zapewnienie cyberbezpieczeństwa dla końcowych beneficjentów tych usług. Raz jeszcze wypada bowiem wskazać, że bezpośrednimi adresatami norm uksc nie są końcowi użytkownicy usług, tylko podmioty wymienione w art. 4 uksc.

Poddając w pierwszym kroku analizie prawnej obowiązki operatorów usług kluczowych, oczywiście z punktu widzenia zapewnienia właściwego poziomu cyberbezpieczeństwa dla beneficjentów tych usług, należy wyjść od zdefiniowania tej kategorii pojęciowej.

Zgodnie z art. 5 ust. 1 uksc, operatorem usługi kluczowej jest podmiot, który został wymieniony (w zakresie kategorii prowadzonej działalności, tj. w zakresie sektora, podsektora oraz typu podmiotu) w załączniku nr 1 do uksc, który to podmiot posiada jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej i wobec którego właściwy organ administracji publicznej (organ właściwy do spraw cyberbezpieczeństwa, tj. organ wskazany w art. 41 uksc) wydał decyzję o uznaniu za operatora usługi kluczowej (tj. usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych w uksc).

Dla uznania danego podmiotu za operatora usług kluczowych konieczne jest zatem kumulatywne spełnienie się trzech warunków: (i) musi być to podmiot, o którym jest mowa w załączniku nr 1 do uksc; (ii) musi być to podmiot, który posiada jednostkę organizacyjną (jak np. spółkę czy oddział) na terytorium Rzeczypospolitej Polskiej (co jest oczywiste, przepisy uksc mają bowiem charakter regulacji publicznoprawnej, a tym samym mają wyłącznie wewnątrzkrajowy zakres zastosowania); (iii) podmiot ten jest adresatem decyzji administracyjnej, o której jest mowa w art. 5 ust. 2 i nast. uksc, przy czym warunkami koniecznymi – których kumulatywne spełnienie się jest konieczne dla wydania tej decyzji – są: że podmiot ten świadczy usługę kluczową (jeśli zatem podmiot, który jest wymieniony załączniku 1 nie świadczy usługi kluczowej, bo np. zaprzestał już trwale jej świadczenia, nie będzie mógł być adresatem takiej decyzji; taka decyzja byłaby bowiem decyzją wydaną z rażącym naruszeniem prawa, co czyniłoby koniecznym zastosowanie wobec niej środka prawnego nadzwyczajnego z art. 156 § 1 pkt 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego); świadczenie tej usługi jest uzależnione od prawidłowego funkcjonowania systemów informacyjnych; ewentualny incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora, co jest określane na podstawie progów istotności skutku zakłócającego incydentu określonych w treści rozporządzenia Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (DzU 2018, poz. 1806) (*argumentum ex* art. 5 ust. 2–7 uksc).

Poddając analizie postanowienia z art. 5 ust. 2–7 uksc, z punktu widzenia usługobiorcy należy wskazać, że prawodawca przyznał bezwzględny prymat w ochronie bezpieczeństwu usług kluczowych (a zatem bezpieczeństwu usługobiorcy), co odbyło się – w pewnym stopniu – kosztem operatora usług kluczowych. Decyzja o uznaniu danego podmiotu za operatora usług kluczowych jest bowiem decyzją natychmiast wykonalną z mocy prawa (*argumentum ex* art. 5 ust. 7 uksc), a tym samym wniesienie przez operatora usług kluczowych środka prawnego od tej decyzji, co do zasady, nie będzie wstrzymywało jej wykonalności. W rezultacie już „nieostateczne" uznanie danego podmiotu przez właściwy organ za operatora usługi kluczowej skutkować będzie tym, że podmiot ten, nawet pomimo wniesienia przez niego środka prawnego zwyczajnego od tej decyzji, podlegać będzie obowiązkom z uksc. W istocie chodzi tutaj bowiem o zapewnienie sytuacji, w której to operatorzy usług kluczowych będą realizować, wynikające z odpowiednich postanowień uksc, obowiązki w obszarze zapewnienia cyberbezpieczeństwa od możliwie najwcześniejszej chwili (tj. od momentu wydania niejako „pierwszoinstancyjnej" decyzji administracyjnej w sprawie

uznania danego podmiotu za operatora usług kluczowych w reżimie uksc). Takie rozwiązanie jest z istotną korzyścią dla beneficjentów usług kluczowych, którzy mogą korzystać z usług kluczowych charakteryzujących się wymaganym prawem poziomem cyberbezpieczeństwa od istotnie wcześniejszej chwili, niżeli miałoby to miejsce w sytuacji, gdyby uznanie danego podmiotu za operatora usług kluczowych w reżimie uksc następowało dopiero w chwili doręczenia albo ogłoszenia decyzji ostatecznej w sprawie. W konsekwencji rozwiązanie to zasługuje, z punktu widzenia potrzeby zapewnienia cyberbezpieczeństwa, na jak najbardziej pozytywną ocenę; mamy bowiem do czynienia z sytuacją, w której to sytuacji ten pożądany stan zapewniany jest (w funkcji czasu) wcześniej, co więcej należy przy tym podkreślić, że podmiot uznany za operatora usług kluczowych zobowiązany jest zastosować się do reżimu uksc nawet w sytuacji skorzystania przez niego ze środka prawnego zwyczajnego.

W tym miejscu należy dodatkowo wskazać, że waga obowiązków w zakresie cyberbezpieczeństwa jest na tyle istotna, że prawodawca w przypadku wyżej powołanej decyzji stosuje środek nadzoru w postaci wygaśnięcia tej decyzji z mocy prawa. I tak w sytuacji, gdy podmiot (operator usługi kluczowej) przestanie spełniać warunki dla uznania go za operatora usług kluczowych właściwy organ administracji publicznej do spraw cyberbezpieczeństwa zobowiązany jest wygasić decyzję administracyjną w sprawie uznania danego podmiotu za operatora usług kluczowych. Zastosowanie takiego rozwiązania wskazuje na intencję prawodawcy odnośnie do sprawowania przez właściwe organy administracji publicznej stałego nadzoru nad tym czy dany podmiot wpisany do wykazu operatorów usług kluczowych spełnia stale wszystkie wymogi do figurowania w tym wykazie. Wykaz ten może być w rezultacie postrzegany jako quasi-rejestr publiczny (jakkolwiek prawodawca nie zdecydował się zapewnić pełnego dostępu do tego rejestru, co będzie przedmiotem poszerzonych rozważań w dalszej części niniejszego dokumentu), a podmioty figurujące w tym wykazie jako podmioty, które powinny cieszyć się powszechną rękojmią zaufania publicznego, jako podmioty gwarantujące odpowiedni (wymagany przepisami uksc) poziom cyberbezpieczeństwa.

Dokonując oceny zastosowania takiego rozwiązania z punktu widzenia końcowego użytkownika (odbiorcy) usług, należy wskazać, że rozwiązanie to zasługuje na jak najbardziej pozytywną ocenę. Użytkownicy mają bowiem swoistą gwarancję, że nadzór nad operatorami usług kluczowych nie jest wyłącznie nadzorem administracyjnym wstępnym (tj. związanym z samym wpisem), lecz jest to jednocześnie nadzór administracyjny bieżący (por. szerzej: art. 53 i nast. uksc) i następczy (tj. związany ze stałą weryfikacją przez właściwe organy administracji publicznej okoliczności spełniania przez danego operatora wymogów określonych w art. 5 ust. 1–2 uksc oraz związany z możliwością wykreślenia podmiotu, który nie spełnia wyżej powołanych wymogów regulacyjnych z tego rejestru). W sytuacji bowiem gdy dany podmiot przestanie być operatorem usług publicznych, okoliczność ta będzie musiała zostać dostrzeżona z urzędu przez właściwy organ administracji publicznej i organ ten będzie zobowiązany odpowiednio zmodyfikować wykaz. W rezultacie wykaz będzie stale aktualny i będzie zawierał wyłącznie te czynne podmioty, które to są operatorami usług publicznych; jednocześnie każdy z tych podmiotów będzie miał pełną świadomość, że właściwe organy administracji publicznej weryfikują działalność tych podmiotów i są uprawnione zastosować, w sytuacji stwierdzenia jakichkolwiek nieprawidłowości, odpowiednie władcze środki nadzoru. W tym miejscu należy jeszcze raz podkreślić, że beneficjentem powyższego rozwiązania

są beneficjenci usług kluczowych oferowanych przez operatora. Podmioty te mogą bowiem zasadnie oczekiwać, że operatorzy usług kluczowych będą zachowywać najwyższy standard w zakresie zapewnienia cyberbezpieczeństwa. Co więcej, w przypadku powstania sporu sądowego pomiędzy beneficjentem a operatorem odnośnie do zachowania przez operatora usług kluczowych odpowiedniego standardu cyberbezpieczeństwa, będzie istniało domniemanie prawne co do prawnej konieczności zachowania przez tego operatora standardu z uksc i to operator będzie zobowiązany wykazać, że standard ten nie musiał być zachowany.

De lege ferenda należałoby zastanowić się czy z punktu widzenia bezpieczeństwa użytkownika końcowego nie byłoby celowym zapewnienie publicznego dostępu do wykazu (a zatem uczynienie z tego wykazu publicznego rejestru) z art. 7 uksc (aktualnie rejestr ten dostępny jest bowiem wyłącznie dla podmiotów określonych w art. 7 ust. 7–8 uksc). Publiczny dostęp do tego wykazu istotnie redukowałby ryzyko tzw. negatywnej selekcji, tj. wyboru przez usługobiorcę usługi kluczowej takiego usługodawcy (operatora usługi kluczowej), który to nie gwarantuje właściwego poziomu cyberbezpieczeństwa. W obliczu zapewnienia publicznego dostępu do tego wykazu każdy usługobiorca mógłby w bardzo łatwy sposób zweryfikować czy usługodawca zapewnia odpowiedni standard cyberbezpieczeństwa, a tym samym czy podmiot ten cieszy się rękojmią zaufania publicznego. Jak się wydaje wdrożenie tego rozwiązania byłoby z istotną korzyścią dla beneficjentów usług kluczowych, w tym kontekście celowe jest odwołanie się do dobrych doświadczeń płynących z innych rejestrów publicznych, jak np. tych prowadzonych przez Komisję Nadzoru Finansowego. I tak na stronie internetowej Komisji Nadzoru Finansowego można w bardzo łatwy sposób zweryfikować czy dany usługodawca (w obszarze usług finansowych) jest podmiotem, który cieszy się odpowiednią rękojmią, czy też jest to raczej podmiot, przed współpracą z którym Komisja Nadzoru Finansowego ostrzega (jak w przypadku Listy ostrzeżeń publicznych).

Przechodząc niejako w kolejnym kroku do analizy obowiązków publicznoprawnych spoczywających na operatorach usług kluczowych i ich oceny z punktu widzenia zapewnienia cyberbezpieczeństwa dla beneficjentów usług kluczowych, należy przede wszystkim wskazać, że obowiązki operatora ogniskują się w następujących obszarach:

1) w zakresie wdrożenia odpowiednich rozwiązań systemowych w obszarze zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej. System ten ma zapewniać:
   (i) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
   (ii) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym: utrzymanie i bezpieczną eksploatację systemu informacyjnego; bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu; bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej; wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji; objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

(iii) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
(iv) zarządzanie incydentami;
(v) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym: stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym; dbałość o aktualizację oprogramowania; ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym; niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa; (vi) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa (*argumentum ex* art. 8 u.k.s.c.);

2) w zakresie odpowiedniej organizacji personelu. I tak operator usługi kluczowej jest zobowiązany wyznaczyć osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (*argumentum ex* art. 9 ust. 1 pkt 1 uksc);
3) w zakresie informowania użytkowników usług. I tak, zgodnie z art. 9 ust. 1 pkt 2 uksc, operator usługi kluczowej jest zobowiązany zapewnić użytkownikowi usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji na ten temat na swojej stronie internetowej;
4) w zakresie informowania właściwego organu do spraw cyberbezpieczeństwa, tak by organ ten dysponował aktualnymi (nie później niż w terminie 3 miesięcy od zmiany tych danych) danymi, o których jest mowa w art. 7 ust. 2 pkt 8 i 9 uksc (*argumentum ex* art. 9 ust. 1 pkt 3 uksc);
5) w zakresie wdrożenia i stosowania odpowiednich procedur. I tak zgodnie z art. 10 uksc operator usługi kluczowej opracowuje, stosuje i aktualizuje dokumentację – zgodnie z postanowieniami rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberzbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (DzU 2018, poz. 2080) – dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej[2]. Operator ten jest przy tym zobowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zapewniającego: dostępność dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami; ochronę dokumentów przed niewłaściwym użyciem lub utratą integralności; oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach. Dodatkowym obowiązkiem operatora jest przechowywanie dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez co najmniej 2 lata od dnia jej wycofania

[2] Przy czym operator usługi kluczowej będący jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU 2018, poz. 1401), który posiada zatwierdzony plan ochrony infrastruktury krytycznej uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, nie ma obowiązku opracowania tej dokumentacji

z użytkowania lub zakończenia świadczenia usługi kluczowej, z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. DzU 2018, poz. 217, ze zm.);

6) w zakresie zapobiegania i odpowiedniej obsługi incydentów (*argumentum ex* art. 11 uksc); w tym w szczególności należy wymienić takie obowiązki operatora usługi kluczowej, jak obowiązek: zapewnienia obsługi incydentu; zapewnienia dostępu do informacji o rejestrowanych incydentach właściwemu podmiotowi publicznemu[3] w zakresie niezbędnym do realizacji jego zadań; klasyfikacji incydentu jako poważny na podstawie progów uznawania incydentu za poważny; niezwłocznego zgłaszania – nie później niż w ciągu 24 godzin od momentu jego wykrycia – incydentu poważnego[4], do właściwego podmiotu publicznego; współdziałania podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym podmiotem publicznym, przekazując niezbędne dane, w tym dane osobowe; usuwania podatności, o których mowa w art. 32 ust. 2 uksc, oraz informowania o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa. Dodatkowo w przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa operator usługi kluczowej zobowiązany jest do: przekazywania jednocześnie temu zespołowi w postaci elektronicznej zgłoszenie dotyczącego incydentu poważnego; współdziałania z tym zespołem na poziomie sektora lub podsektora podczas obsługi incydentu poważnego lub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe; zapewnienie temu zespołowi dostępu do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań;

7) w zakresie przekazywania do właściwego podmiotu publicznego informacji[5] o: innych incydentach; zagrożeniach cyberbezpieczeństwa; dotyczących szacowania ryzyka; podatnościach; wykorzystywanych technologiach (*argumentum ex* art. 13 uksc). W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa operator usługi kluczowej jest uprawniony przekazywać te informacje jednocześnie temu zespołowi.

8) w zakresie powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub w zakresie zawarcia umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (*argumentum ex* art. 14 uksc), co ma zapewnić spełnienie następujących warunków (dookreślonych w treści rozporządzenia Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi

[3] Przez pojęcie to należy rozumieć w treści niniejszego dokumentu takie podmioty, zdefiniowane w uksc, jak CSIRT MON, CSIRT NASK lub CSIRT GOV.

[4] Zgłoszenie to przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji Zgłoszenie to zawiera: dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres; imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia; imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji; opis wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym: usługi kluczowe zgłaszającego, na które incydent poważny miał wpływ, liczbę użytkowników usługi kluczowej, na których incydent poważny miał wpływ, moment wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania, zasięg geograficzny obszaru, którego dotyczy incydent poważny, wpływ incydentu poważnego na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych, przyczynę zaistnienia incydentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe; informacje umożliwiające właściwemu podmiotowi określenie, czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej; w przypadku incydentu, który mógł mieć wpływ na świadczenie usługi kluczowej, opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne; informacje o podjętych działaniach zapobiegawczych; informacje o podjętych działaniach naprawczych; inne istotne informacje. W zakresie informacji wskazanych powyżej mieścić się mogą jak najbardziej informacje stanowiące tajemnice prawnie chronione, w tym te stanowiące tajemnicę przedsiębiorstwa. W zgłoszeniu operator usługi kluczowej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. Operator zobowiązany jest przekazać informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu poważnego. Właściwy podmiot może zwrócić się do operatora usługi kluczowej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

[5] Informacje te przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji. Operator usługi kluczowej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

z zakresie cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo (DzU 2018, poz. 1780)): spełnienie warunków organizacyjnych i technicznych pozwalających na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej; dysponowanie pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi; stosowanie zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

9) w zakresie przeprowadzenie, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, który to audyt musi być przeprowadzony przez uprawnionego audytora (*argumentum ex* art. 15 ust. 2 uksc).

Już bardzo wstępna analiza powyższego katalogu z punktu widzenia potrzeby zapewnienia cyberbezpieczeństwa dla beneficjentów usług kluczowych prowadzi do sformułowania konkluzji, że katalog ten jest bardzo rozbudowany i obejmuje organizację oraz funkcjonowanie operatora usług publicznych. Nie mamy tutaj zatem do czynienia z sytuacją, w której to na operatora usług publicznych zostałby nałożony pojedynczy obowiązek z obszaru cyberbezpieczeństwa, ale z sytuacją, w ramach której prawodawca stawia wobec tego operatora liczne wymogi organizacyjne i funkcjonalne. W konsekwencji z powodzeniem można przyjąć, że prawodawca niejako oczekuje od operatorów usług kluczowych swoistej przebudowy ich działalności operacyjnej i strategicznej w kierunku zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Prawodawca przyjął zatem podejście całościowe, holistyczne; co powinno być uznane za zabieg jak najbardziej celowy i z pozytywnym przełożeniem na zapewnienie odpowiedniego poziomu cyberbezpieczeństwa.

Zabezpieczeniem realizacji powołanych wyżej obowiązków i niejako klamrą spinającą powyższy katalog jest mechanizm nadzoru z art. 53–59 uksc i ściśle z nim powiązany mechanizm odpowiedzialności administracyjnej z art. 73 i nast. uksc. I tak w ramach nadzoru właściwy organ prowadzi kontrole oraz nakłada kary pieniężne na operatorów usług kluczowych. W tym kontekście należy wyraźnie podkreślić to, że wybór przez krajowego prawodawcę sankcji administracyjnej (administracyjnej kary pieniężnej) jako mechanizmu zabezpieczającego realizację obowiązków publicznoprawnych jest zabiegiem słusznym.

Kara administracyjna, w mojej ocenie, jest bowiem w praktyce obrotu gospodarczego dużo bardziej efektywnym instrumentem oddziaływania niż klasyczna kara wywodząca się z gałęzi prawa karnego. W praktyce bowiem kara administracyjna znajduje zastosowanie w krótszym czasie, aniżeli ma to miejsce w przypadku klasycznych instrumentów odpowiedzialności karnej, co więcej to kara administracyjna znajduje statystycznie – nawet w sytuacji, gdy dany delikt zagrożony jest sankcjami tak administracyjną, jak i karną – zastosowanie dużo częściej. Czytelnym potwierdzeniem powyższego zjawiska jest tendencja, która aktualnie widoczna jest w krajowym i unijnym porządku normatywnym, która to tendencja wyraża się w zastępowaniu mechanizmów odpowiedzialności karnej mechanizmami odpowiedzialności administracyjnej (zob. np. ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu).

O tej swoistej przewadze kar administracyjnych jako instrumentu lepiej zabezpieczającego wykonywanie obowiązków publicznoprawnych przemawia też argument natury pragmatycznej. Autorowi niniejszego opracowania znane są przykłady deliktów, wobec których to kara

administracyjna znalazła jak najbardziej zastosowanie, a prowadzone postępowanie karne nie zakończyło się bynajmniej zastosowaniem kary właściwej dla prawa karnego czy to z uwagi na niemożność stwierdzenia popełnienia deliktu w postępowaniu sądowym, czy za względu na przedawnienie odpowiedzialności karnej.

Stanowi to, jak się wydaje, istotny argument przemawiający za przyjęciem stanowiska, że wybór przez prawodawcę w reżimie uksc odpowiedzialności administracyjnej jako mechanizmu zabezpieczającego realizację obowiązków publicznoprawnych jest wyborem trafnym i z jak najbardziej pozytywnym przełożeniem na zapewnienie odpowiedniego poziomu cyberbezpieczeństwa dla beneficjentów usług kluczowych.

Należy przy tym wyraźnie wskazać to, że zabezpieczenie realizacji wyżej powołanych obowiązków z wykorzystaniem mechanizmu odpowiedzialności administracyjnej jest działaniem, które leży w interesie usługobiorców; praktyczna skuteczność mechanizmu odpowiedzialności administracyjnej stanowi bowiem gwarancję, że obowiązki te będą faktycznie realizowane. Można bowiem zasadnie domniemywać, że operatorzy usług publicznych, mając na uwadze okoliczność nieuchronności odpowiedzialności administracyjnej w przypadku wystąpienia tzw. deliktu administracyjnego, będą przywiązywali szczególną wagę do kwestii zapewnienia cyberbezpieczeństwa, co będzie miało jak najbardziej pozytywne przełożenie na zapewnienie cyberbezpieczeństwa dla beneficjentów usług kluczowych.

Dokonując analizy katalogu obowiązków operatora usług publicznych z punktu widzenia usługobiorców usługi kluczowej (tj. beneficjentów tych usług), należy wskazać, że wszystkie te obowiązki skoncentrowane są na zapewnieniu wymaganego prawem poziomu cyberbezpieczeństwa usługi kluczowej. *Ratio legis* wprowadzenia powyższego obowiązku ustawowego jest zatem zapewnienie cyberbezpieczeństwa dla beneficjenta usługi kluczowej, która to wartość musi być postrzegana w rezultacie jako wartość dominująca i kluczowa. Na uwagę i kilka zdań komentarza zasługuje fakt, że intencją prawodawcy jest by cyberbezpieczeństwo usługi było zapewniane tak na poziomie operacyjnym (tj. na poziomie realizacji usługi), jak i na poziomie strategicznym (tj. na poziomie organizacji operatora usługi kluczowej). Obowiązki spoczywające na operatorze usługi kluczowej ogniskują się bowiem zarównow obszarze organizacji wewnętrznej struktury i procesów zachodzących w ramach operatora, jak i w obszarze pojedynczych operacji podejmowanych przez tego operatora.

W ujęciu teoretycznoprawnym należy zatem uznać przyjęte przez krajowego prawodawcę rozwiązanie za właściwe jako pełne, a obrany model regulacji za model holistyczny i całościowy. Jest to z niewątpliwą korzyścią dla beneficjentów tych usług, pozwala bowiem uniknąć sytuacji, w której to rozwiązanie wprowadzone w sferze funkcjonalnej nie mogłyby prawidłowo działać z uwagi na brak odpowiednich dostosowań organizacyjnych.

Rozwiązanie to, jakkolwiek jest relatywnie nowe (jego historia nie obejmuje nawet 1 roku), zasługuje na pozytywną ocenę również w ujęciu praktycznoprawnym. W okresie jego obowiązywania nie mieliśmy bowiem, zgodnie z moją najlepszą wiedzą i informacjami dostępnymi w domenie publicznej, do czynienia z chociażby pojedynczym incydentem istotnym, który to incydent zakłóciłby możliwość świadczenia usług kluczowych, gdzie równolegle do kategorii notorii powszechnych należy wiadomość, że taki incydent miał miejsce kilka miesięcy temu w Estonii i doprowadził do czasowego zablokowania możliwości świadczenia usług kluczowych przez tamtejsze organy e-administracji.

Konkludując, należy wskazać, że wynikające z odpowiednich postanowień uksc rozwiązania normatywne dotyczące cyberbezpieczeństwa w zakresie działalności operatorów usług kluczowych zasługują, z punktu widzenia zapewnienia cyberbezpieczeństwa dla obywateli, na jak najbardziej pozytywną ocenę. Rozwiązania te pozwalają bowiem końcowym beneficjentom usług kluczowych korzystać z usług charakteryzujących się odpowiednim poziomem cyberbezpieczeństwa, a tym samym pozwalają one ograniczyć ryzyko związane z usługami kluczowymi. Warto w tym miejscu raz jeszcze wskazać, że jest to z korzyścią tak dla beneficjentów tych usług, jak i dla operatorów usług kluczowych; pozwala bowiem uniknąć sytuacji, w której to beneficjenci nie korzystają z usług kluczowych z uwagi na ryzyko w obszarze cyberbezpieczeństwa.

IV. Obowiązki dostawców usług cyfrowych

Dokonując analizy obowiązków dostawców usług cyfrowych z punktu widzenia zapewnienia wymaganego prawem poziomu ochrony i cyberbezpieczeństwa dla beneficjentów tych usług, a tym samym z punktu widzenia ochrony beneficjentów, należy podobnie wyjść od zdefiniowania pojęcia „dostawca usług cyfrowych".

Zgodnie z art. 17 ust. 1 uksc, dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej, albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową, o której jest mowa w załączniku nr 2 do uksc, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (DzU 2018, poz. 646, ze zm.).

Dla uznania danego podmiotu za dostawcę usług cyfrowych konieczne jest zatem kumulatywne spełnienie się dwóch warunków: (i) musi być to podmiot, który jest osobą prawną albo jednostką organizacyjną nieposiadającą osobowości prawnej mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, przy czym nie może być to jednocześnie mikroprzedsiębiorca i mały przedsiębiorca, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców; (ii) podmiot ten musi świadczyć usługę cyfrową, o której to usłudze jest mowa w załączniku nr 2 do uksc.

Już bardzo pobieżne zestawienie ze sobą definicji legalnej operatora usług kluczowych i dostawcy usług cyfrowych prowadzi do sformułowania konkluzji, że wymogi regulacyjne formułowane wobec tego pierwszego podmiotu są bardziej rozbudowane i wymagające, niżeli wymogi formułowane przez prawodawcę krajowego wobec dostawcy usług cyfrowych. *Ratio* takiego rozróżnienia wymogów regulacyjnych było, jak się wydaje,, że w przypadku operatorów usług kluczowych ryzyko związane z tymi usługami – z punktu widzenia tak interesu społecznego, interesu ekonomicznego systemu gospodarczego, jak i interesu końcowego użytkownika usługi (beneficjenta usługi) – jest istotnie wyższe, niżeli ma to miejsce w przypadku ryzyka związanego z usługami cyfrowymi. Te pierwsze usługi mają bowiem ze swojej natury fundamentalny wpływ na funkcjonowanie systemu gospodarczego i jakiekolwiek nieprawidłowości w tym obszarze mogą mieć szczególnie doniosłe konsekwencje gospodarcze (można sobie bowiem wyobrazić sytuację, w której w rezultacie incydentu istotnego w zakresie cyberbezpieczeństwa przestaje funkcjonować sieć energetyczna, co skutkowałoby czasowym „zatrzymaniem" całego systemu gospodarczego). W przypadku tych

drugich usług krąg osób eksponowanych na ryzyko jest natomiast istotnie mniejszy. Swoistą ofiarą naruszeń w zakresie cyberbezpieczeństwa usług cyfrowych jest bowiem dany korzystający z tej usług usługobiorca, a nie wszyscy usługobiorcy, jak ma to miejsce w przypadku usług kluczowych. W przypadku usług cyfrowych nie mamy bowiem do czynienia, co do zasady, z występowaniem tzw. efektu zarażenia.

Nie bez znaczenia jest również tutaj okoliczność, że w przypadku usług cyfrowych katalog podmiotów świadczących te usługi jest zdecydowanie bardziej rozbudowany, aniżeli ma to miejsce w przypadku usług kluczowych. W konsekwencji niemożliwym było zastosowanie przez prawodawcę rozwiązania sprowadzającego się czy to do stworzenia definicji dostawcy usług cyfrowych opartej na wyliczeniu kategorii podmiotów wchodzących do zbioru desygnatów tego pojęcia (tj. definicji przez wyliczenie), czy też do poddania tej kategorii nadzorowi wstępnemu (w postaci konieczności uzyskania, jak ma to miejsce w przypadku operatorów usług kluczowych, decyzji administracyjnej i odpowiedniego wpisu do wykazu). Usługi cyfrowe mogą być bowiem oferowane przez wszystkie podmioty; tym samym poddanie wszystkich dostawców tych usług nadzorowi wstępnemu byłoby po prostu niewykonalne.

Konsekwencją powyższego jest również, że na dostawców usług cyfrowych prawodawca krajowy nałożył mniejszy zakres obowiązków niż w przypadku operatora usług kluczowych. W tym miejscu należy wskazać, że jakkolwiek takie rozróżnienie może budzić obawy z punktu widzenia potrzeby zapewnienia odpowiedniego cyberbezpieczeństwa, to bliższe przyjrzenie się prowadzi do sformułowania konkluzji, że mamy tutaj do czynienia z rozwiązaniem celowym. Należy bowiem przypomnieć, że ochrona w reżimie uksc odbywa się wyłącznie w sposób pośredni, tj. poprzez nałożenie odpowiednich obowiązków na operatorów usług kluczowych i na dostawców usług cyfrowych. Czysto hipotetycznie można sobie wyobrazić sytuację, w której to operatorzy usług kluczowych i dostawcy usług cyfrowych podlegaliby tożsamym obowiązkom w zakresie cyberbezpieczeństwa, w ujęciu praktycznym prowadziłoby to jednak do wystąpienia sytuacji, w której usługi cyfrowe byłyby trudniej dostępne. Konieczność spełnienia przez ich dostawców rozbudowanego zestawu obowiązków, które to obowiązki byłyby tożsame z obowiązkami spoczywającymi na operatorach usług kluczowych, istotnie redukowałoby bowiem atrakcyjność ekonomiczną świadczenia usług cyfrowych, czyniąc te usługi drogimi. W rezultacie mielibyśmy do czynienia z sytuacją, w której usługi cyfrowe nie byłyby świadczone (z uwagi na brak popytu na nie) czy też byłyby świadczone w zdecydowanie mniejszym wymiarze niż ma to miejsce aktualnie.

Punktem wspólnym łączącym oba te katalogi obowiązków jest fakt, że są one zawsze skoncentrowane na zapewnieniu cyfrowego bezpieczeństwa (cyberbezpieczeństwa) świadczonych usług, co jest z niewątpliwą korzyścią dla końcowego beneficjenta tych usług. Jak zostało to bowiem wskazane, to cyberbezpieczeństwo jest zasadniczym *ratio* regulacji z uksc.

Wypada przy tym nadmienić, że w przypadku dostawców usług cyfrowych katalog ich obowiązków został skonstruowany w oparciu o realizację postanowień płynących z zasady proporcjonalności. Dostawca usług cyfrowych zobowiązany jest bowiem dostosować zakres i charakter spoczywających na nim obowiązków z uksc do specyfiki prowadzonej przez siebie działalności gospodarczej. Dostawca ten został zobowiązany, na mocy postanowień z art. 17 ust. 2 uksc, do podejmowania właściwych i proporcjonalnych środków technicznych i organizacyjnych określonych w rozporządzeniu wykonawczym 2018/151 w celu zarządzania ryzykiem, na jakie narażone są

systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te mają zapewnić cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniać: bezpieczeństwo systemów informacyjnych i obiektów; postępowanie w przypadku obsługi incydentu; zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej; monitorowanie, audyt i testowanie; najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2018/151. Dodatkowo dostawca usługi cyfrowej został zobowiązany do podejmowania środków zapobiegających i minimalizujących wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi.

W ramach realizacji wyżej powołanych obowiązków dostawca zobowiązany jest (*argumentum ex* art. 18 uksc) do: przeprowadzania czynności umożliwiających wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów; zapewnienia w niezbędnym zakresie dostępu do informacji dla właściwego podmiotu publicznego o incydentach zakwalifikowanych jako krytyczne przez właściwy podmiot publiczny; klasyfikowania incydentów jako istotnych; zgłaszania incydentów istotnych[6] niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego podmiotu publicznego; zapewnienia obsługi incydentu istotnego i incydentu krytycznego we współpracy z właściwym podmiotem publicznym, przekazując niezbędne dane, w tym dane osobowe; usuwania podatności, o których mowa w art. 32 ust. 2 uksc; przekazywania operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacji dotyczącej incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora.

Należy przy tym wskazać, że zgodnie z art. 20 uksc dostawca usługi cyfrowej może (a zatem jest do tego wyłącznie uprawniony, a nie zobowiązany; tym samym realizacji postanowień tego przepisu odbywać się będzie na zasadzie fakultatywności) przekazywać do właściwego podmiotu publicznego informacje, o innych incydentach; o zagrożeniach cyberbezpieczeństwa; dotyczące szacowania ryzyka; o podatnościach; o wykorzystywanych technologiach. Informacje te przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania ich w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Zestawienie ze sobą katalogu obowiązków operatora usług kluczowych z katalogiem obowiązków dostawcy usług cyfrowych prowadzi do sformułowania dwóch istotnych, z punktu widzenia tematu niniejszego opracowania, konkluzji.

[6] Zgłoszenie incydentu przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji. Jednakże dostawca usługi cyfrowej nie ma obowiązku dokonania zgłoszenia, gdy nie posiada informacji pozwalających na ocenę istotności wpływu incydentu na świadczenie usługi cyfrowej. Dostawca usługi cyfrowej, klasyfikując incydent jako istotny, ocenia istotność wpływu incydentu na świadczenie usługi cyfrowej na podstawie niżej powołanych parametrów oraz progów określonych w rozporządzeniu wykonawczym 2018/151. Dostawca usługi cyfrowej w celu sklasyfikowania incydentu jako istotnego uwzględnia w szczególności następujące parametry: liczba użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług; czas trwania incydentu; zasięg geograficzny obszaru, którego dotyczy incydent; zakres zakłócenia funkcjonowania usługi; zakres wpływu incydentu na działalność gospodarczą i społeczną.
Zgłoszenie to zawiera: dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres; imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie; imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji; opis wpływu incydentu istotnego na świadczenie usługi cyfrowej, w tym: liczbę użytkowników, na których incydent istotny miał wpływ, moment wystąpienia i wykrycia incydentu istotnego oraz czas jego trwania, zasięg geograficzny obszaru, którego dotyczy incydent istotny, zakres zakłócenia funkcjonowania usługi cyfrowej, zakres wpływu incydentu istotnego na działalność gospodarczą i społeczną; informacje umożliwiające właściwemu podmiotowi publicznemu określenie, czy incydent istotny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej; informacje o przyczynie i źródle incydentu istotnego; informacje o podjętych działaniach zapobiegawczych; informacje o podjętych działaniach naprawczych; inne istotne informacje. Dostawca usługi cyfrowej przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które następnie uzupełnia w trakcie obsługi incydentu istotnego. W zgłoszeniu dostawcy usług cyfrowych oznaczają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. Dostawca usługi cyfrowej przekazuje, w niezbędnym zakresie, w zgłoszeniu informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego podmiotu publicznego. Właściwy podmiot publiczny może zwrócić się do dostawcy usługi cyfrowej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w uksc.

Po pierwsze, w przypadku katalogu obowiązków dostawcy usług cyfrowych jego konstrukcja została oparta na zasadzie proporcjonalności (*argumentum ex* art. 17 ust. 2 uksc). Tym samym katalog ten jest w istocie katalogiem *szytym na miarę,* tj. katalog ten musi być w maksymalnym stopniu dopasowany do specyfiki funkcjonowania (specyfiki świadczonych usług) danego dostawcy usług cyfrowych.

Rozwiązanie to należy uznać za w pełni zasadne i celowe, gwarantuje ono bowiem, że katalog obowiązków będzie w każdym przypadku idealnie dopasowany do specyfiki działalności danego dostawcy, a tym samym, że dostawca ten nie będzie podlegał obowiązkom zbędnym oraz że będzie on podlegał obowiązkom zapewniającym faktycznie cyberbezpieczeństwo, nie zaś obowiązkom, których realizacja nie prowadzi do wypracowania tego rezultatu, a tym samym niejako „zbędnym" obowiązkom. Ma to przy tym pozytywne przełożenie na cyberbezpieczeństwo, prowadzi bowiem do wystąpienia sytuacji, w której to poziom wymogów formułowanych przez prawodawcę w odniesieniu do dostawcy usług cyfrowych jest idealnie dopasowany do specyfiki prowadzonej działalności, a tym samym nie stanowi on nadmiernego obciążenia, a jednocześnie zapewniony jest odpowiedni, wymagany przez beneficjentów usług cyfrowych, poziom cyberbezpieczeństwa.

Za oparciem katalogu obowiązków dostawcy usług cyfrowych na zasadzie proporcjonalności przemawiało dodatkowo, że grupa dostawców usług cyfrowych i katalog usług cyfrowych są bardzo rozbudowane, a tym samym wręcz niemożliwe byłoby stworzenie kazuistycznego katalogu tych obowiązków, który to treść jest funkcją realizowanej usługi cyfrowej.

Po drugie, co jest bezpośrednim wynikiem przyjętej przez prawodawcę koncepcji odnośnie do proporcjonalności obowiązków dostawcy usług cyfrowych, katalog ten jest istotnie mniej rozbudowany, aniżeli w przypadku katalogu obowiązków operatora usług kluczowych. Rozwiązanie to jest oczywiście wynikiem tego, że poziom ryzyka (tj. zagrożenia dla interesu społecznego i systemu gospodarczego) w przypadku tych usług jest istotnie niższy niż w przypadku usług kluczowych. Może być bowiem tak, że przykładowo zakłócenia w zakresie cyberbezpieczeństwa w ramach działalności jednego banku krajowego, w rozumieniu przepisów ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, mogą w rezultacie tzw. efektu zarażenia, prowadzić do wystąpienia zakłóceń w zakresie funkcjonowania innych banków krajowych, a nawet do wystąpienia stanu zagrożenia dla całego systemu bankowego.

W przypadku obowiązków dostawcy usług cyfrowych ich realizacja została, podobnie jak miało to miejsce w przypadku obowiązków operatora usług kluczowych, zabezpieczona z wykorzystaniem mechanizmu nadzoru w połączeniu z wykorzystaniem mechanizmu odpowiedzialności administracyjnej (*argumentum ex* art. 53–59 oraz z art. 73 i nast. uksc). Rozwiązanie to, z tożsamych przyczyn jak w przypadku nadzoru administracyjnego nad realizacją przez operatora usług kluczowych jego obowiązków, zasługuje również na pozytywną ocenę jako rozwiązanie, które w najlepszy sposób chroni interesy beneficjentów usług cyfrowych. Ci ostatni mogą być bowiem pewni, że jakikolwiek delikt administracyjny w obszarze respektowania przez dostawcę usług cyfrowych norm uksc, spotka się z odpowiednią władczą reakcją właściwego organu administracji publicznej.

Dokonując oceny scharakteryzowanych powyżej mechanizmów i rozwiązań z punktu widzenia potrzeby zapewnienia cyberbezpieczeństwa dla beneficjentów usług cyfrowych, należy wskazać, że zasługują one na pozytywną ocenę.

W szczególności pozytywnie należy odnieść się do przyjętej przez krajowego prawodawcę koncepcji oparcia katalogu obowiązków dostawcy usług cyfrowych na zasadzie proporcjonalności, która to koncepcja stanowi swoistą gwarancję, że dostawca usług cyfrowych będzie podlegał wyłącznie takiej grupie obowiązków publicznoprawnych, które będą pozwalały na zapewnienie cyberbezpieczeństwa oferowanych usług cyfrowych, a jednocześnie nie będą stanowiły one niepotrzebnego obciążenia dla tego dostawcy. W tym ostatnim kontekście celowe jest przypomnienie, że z punktu widzenia adresata obowiązku każdy obowiązek publicznoprawny jest kosztem, który to obciąża wyniki finansowe wypracowywane przez tego adresata; przy czym mamy tutaj do czynienia z obciążeniem podwójnym, tj. raz w związku z koniecznością dopasowania prowadzonej działalności do tego obowiązku, drugi – w związku z wprowadzeniem ograniczeń regulacyjnych, które to ograniczenia prowadzą do zredukowania możliwego do podjęcia ryzyka, a tym samym do ograniczenia rentowności prowadzonej działalności.

V. Podsumowanie

Regulacja uksc jest z całą pewnością specyficzną regulacją gospodarczą, którą można –zaliczyć do tzw. regulacji sektorowej (za: Skoczny, 2013, s. 1359–1362; Walulik, 2013, s. 67). *Ratio* tej regulacji nie jest bowiem, co można uznać za rozwiązanie klasyczne dla regulacji gospodarczej, zapewnienie prokonkurencyjnego rynku, ale zagwarantowanie bezpieczeństwa technicznego infrastruktury cyfrowej. Normy uksc mogą być zatem z powodzeniem zaliczone nie tyle do regulacji ekonomicznej, nakierowanej na wspieranie mechanizmu konkurencji, ile do regulacji społecznej, która związana jest z zapewnieniem bezpieczeństwa.

O wskazanej wyżej specyfice świadczy też niezwykle interesujący, obrany przez prawodawców unijnego i krajowego, model wypracowania powyższego celu regulacyjnego. W powyższym kontekście należy wskazać, że jakkolwiek użytkownicy usług kluczowych i usług cyfrowych (beneficjenci tych usług) nie są, co zostało szczegółowo wskazane w treści niniejszego opracowania, bezpośrednim adresatem (nie mieszczą się w zakresie podmiotowym) regulacji z uksc, to ustawa ta ma istotny i szczególny wpływ na zapewnienie właśnie cyberbezpieczeństwa dla wszystkich beneficjentów usług kluczowych i cyfrowych. Mamy zatem do czynienia z realizacją celu regulacyjnego na szczeblu mikro (tj. z faktycznym zapewnieniem cyberbezpieczeństwa), poprzez oddziaływanie na rynek na szczeblu makro. Prawodawca, nakładając obowiązki w obszarze cyberbezpieczeństwa na operatorów usług kluczowych i na dostawców usług cyfrowych zapewnił dzięki temu, że oferowane usługi kluczowe i cyfrowe będą prawidłowe i cyberbezpieczne, co ma swoje bezpośrednie przełożenie na poziom cyberbezpieczeństwa dla końcowych beneficjentów tych usług.

Mamy zatem do czynienia z klasycznym rozwiązaniem, w ramach którego obowiązek jednego podmiotu (tj. podmiotów wymienionych z art. 4 uksc) jest skorelowany z uprawnieniem innego podmiotu (tj. beneficjentów usług kluczowych i usług cyfrowych), w tym wypadku z uprawnieniem w zakresie korzystania z cyberbezpiecznych i prawidłowych usług kluczowych i cyfrowych, które to usługi są konieczne dla prawidłowego, stabilnego i bezpiecznego funkcjonowania całego systemu gospodarczego. W tym miejscu celowe jest raz jeszcze podkreślenie, że niezawodność i bezpieczeństwo sieci mają zasadnicze znaczenie dla działalności gospodarczej i społecznej, w szczególności dla funkcjonowania całego jednolitego rynku wewnętrznego. Beneficjenci mogą

w rezultacie z powodzeniem korzystać z efektów rewolucji cyfrowej i w sposób bezpieczny przeprowadzać operacje w ramach sieci opartych na przesyle danych.

Rozwiązania przyjęte czy to na gruncie 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 (Dz. Urz. UE L 194 z 19.07.2016, s. 1), czy to na gruncie, stanowiącej krajową implementację tej dyrektywy, uksc, należy w mojej ocenie ocenić jako dobre, a przy tym przede wszystkim celowe, a zatem jako takie, które faktycznie mogą oddziaływać na zapewnienie cyberbezpieczeństwa świadczonych usług kluczowych i usług cyfrowych.

Należy jednak krytycznie odnieść się do okoliczności, że wykaz operatorów usług kluczowych z art. uksc nie jest wykazem dostępnym publicznie. Jak się wydaje, możliwość uzyskania przez końcowych użytkowników usług kluczowych dostępu do tego wykazu przełożyłaby się na zmniejszenie ryzyka dokonania tzw. negatywnej selekcji. Użytkownicy ci mogliby bowiem w bardzo łatwy sposób zweryfikować czy dany operator usługi kluczowej działa prawidłowo i właściwie realizuje spoczywające na nim obowiązki w zakresie zapewnienia cyberbezpieczeństwa. *De lege ferenda* należy zatem postulować wprowadzenie odpowiedniej zmiany do treści uksc, która to zmiana przełoży się na dalsze zwiększenie poziomu cyberbezpieczeństwa dla końcowych beneficjentów usług kluczowych.

Bibliografia

Długosz, T. (2013). Funkcja regulacyjna. W: R. Hauser, Z. Niewiadomski, A. Wróbel (red.), *Publiczne prawo gospodarcze. System prawa administracyjnego* (t. 8a). Warszawa: Wydawnictwo C.H. Beck.

Hoff, W. (2008). *Prawny model regulacji sektorowej.* Warszawa: Centrum Doradztwa i Informacji, Difin.

Skoczny, T. (2013). Regulacja prokonkurencyjna w sektorach infrastrukturalnych. W: M. Kępiński (red.), *Prawo konkurencji. System Prawa Prywatnego.* Warszawa: Wydawnictwo C.H. Beck.

Strzyczkowski, K. (2010). *Prawo gospodarcze publiczne.* Warszawa: LexisNexis.

Walulik, J. (2013). *Reforma regulacyjna. Przykład transportu lotniczego.* Warszawa: Wydawnictwo EuroPrawo.