Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom

r.pr. *Marta Kruk*[1]

Celem niniejszego opracowania jest usystematyzowanie oraz analiza obowiązków dostawców usług cyfrowych wynikających z przepisów o krajowym systemie cyberbezpieczeństwa. W opracowaniu skupiono się także na wskazaniu, jakie podmioty są uznawane za dostawców usług cyfrowych w rozumieniu tej ustawy. Analizy obowiązków dokonano, odwołując się do odpowiednich przepisów prawa unijnego. Zwrócono także uwagę na odmienności w zakresie koniecznych do zrealizowania obowiązków związanych z wystąpieniem zdarzeń mogących mieć negatywny wpływ na cyberbezpieczeństwo wynikające z kwalifikacji takich incydentów jako istotne czy krytyczne oraz na kary, jakie mogą wiązać się z niedopełnieniem przez dostawców usług cyfrowych obowiązków wynikających z ustawy.

Uwagi wstępne

Ponad 55% ludności na całym świecie korzysta obecnie z Internetu, przy czym w samej Europie wskaźnik ten wynosi 85%. Statystyki prowadzone od 2000 r. pokazują stały wzrost w tej dziedzinie[2]. Przyczyną tego zjawiska jest ciągły rozwój świata nowych technologii w świecie cyfrowym, gdzie kolejne nowości innowacyjne i technologiczne stają się codziennością życia. Tendencja ta powoduje, że za główny kierunek rozwoju i wzrostu gospodarczego UE uznano stworzenie jednolitego rynku cyfrowego. Zakłada on wykorzystanie w cyberprzestrzeni nowych technologii takich jak Internet rzeczy (IoT), łączność 5G, przetwarzanie danych i informacji w chmurze czy też dzięki technologiom *big data*[3].

Dynamiczny rozwój nowych technologii cyfrowych stał się podstawą wyodrębnienia cyberbezpieczeństwa jako nowej i samodzielnej dyscypliny naukowej, której nie można analizować wyłącznie w kategoriach technologicznych[4]. Immanentną częścią ekosystemu cyberbezpieczeństwa są bowiem kategorie organizacyjne, ekonomiczne, prawne, społeczne czy współpracy międzynarodowej o zasięgu globalnym[5]. Wykorzystywanie nowych technologii niewątpliwie niesie za sobą korzyści, ale też powoduje liczne i ulegające ciągłej przemianie zagrożenia dla poszczególnych osób fizycznych i prawnych, ogółu ludności, instytucji czy państw. Z jednej strony, skala incydentów w cyberprzestrzeni i ich skutki powodują olbrzymie straty zarówno w gospodarkach państw europejskich, jak i w prowadzonej działalności gospodarczej w sektorze prywatnym, czy też poważne zagrożenie dla zdrowia i mienia obywateli UE[6]. Ryzyko związane z cyberprzestępczością systematycznie wzrasta, powodując podważenie zaufania osób fizycznych do nowych technologii w świecie cyfrowym[7].

Z drugiej strony, nie ma już możliwości odwrotu z obranej drogi rozwoju i odcięcia się czy rezygnacji z wykorzystywania nowych technologii czy to przez rządy państw, w rozwoju gospodarki, w sektorze użyteczności publicznej, sektorze prywatnym czy wreszcie w bieżącym życiu przez osoby fizyczne. Stąd konieczne jest zagwarantowanie bezpieczeństwa obywatelom UE w coraz bardziej obecnej w codziennym życiu cyberprzestrzeni. Ponieważ skala i rodzaje cyberprzestępstw nieustannie ewoluują, pamiętać należy, że nie jest możliwe zapewnienie w 100% odpornych na zagrożenia systemów teleinformatycznych czy też 100% idealnych rozwiązań organizacyjno-prawnych. Odpowiedzialność za zapewnienie cyberbezpieczeństwa obywatelom nie może spoczywać wyłącznie na rządach państw UE, ponieważ cyfrowego świata nie kontroluje wyłącznie sektor publiczny[8]. Aby osiągnąć zakła-

[1] Autorka jest partnerem Kancelarii Prawnej VenaGroup we Wrocławiu oraz rzecznikiem prasowym Okręgowej Izby Radców Prawnych we Wrocławiu.

[2] Zob. https://www.internetworldstats.com/stats.htm (dostęp z 23.1.2019 r.).

[3] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia jednolitego rynku cyfrowego dla Europy", COM(2015) 192 final.

[4] *C. Banasiński*, Cyberbezpieczeństwo w Unii Europejskiej – kierunki regulacji, [w:] *J. Jagielski*, *D. Kijowski* (red.), Prawo administracyjne wobec współczesnych wyzwań. Księga jubileuszowa dedykowana profesorowi Markowi Wierzbowskiemu, Legalis/el. 2018.

[5] *M. Olszewska*, Cyberbezpieczeństwo jako przedmiot analizy przestrzennej, [w:] *G. Szpor*, *K. Czaplicki* (red.), Internet. Informacja przestrzenna. Spatial information, Legalis/el. 2018.

[6] *M.-T. Holzleitner*, *J. Reichl*, European provisions for cyber security in the smart grid – an overview of the NIS-directive, [w:] Elektrotechnik & Informationstechnik, Springer Verlag Wien 2017.

[7] *S. Kotecka*, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, [w:] *J. Gołaczyński* (red.), Wybrane dobre praktyki w zakresie usług elektronicznych, Legalis/el. 2016.

[8] *M. Olszewska*, Cyberbezpieczeństwo jako przedmiot analizy przestrzennej, Legalis/el. 2018.

dany cel, niezbędne jest zaangażowanie sektora prywatnego oraz osób fizycznych[9]. Większość elementów sieci i systemów teleinformatycznych związanych chociażby z tworzeniem, zarządzaniem i rozwojem Internetu czy też część istotnej infrastruktury krytycznej należy do sektora prywatnego. Zasadnicza jest więc zwiększona odpowiedzialność sektora prywatnego i jego zaangażowanie w zapewnienie bezpieczeństwa w cyberprzestrzeni[10]. Pamiętać należy, że równie istotny jest aspekt informacyjny i edukacja konsumentów związana z ich aktywnością w świecie cyfrowym oraz dotyczącym tej aktywności zagrożeniem cyberprzestępstwami[11].

Z powyższych rozważań wynika, że skoro nie jest możliwa całkowita eliminacja zagrożeń związanych z cyberprzestępczością, jedynym słusznym rozwiązaniem jest podjęcie działań minimalizujących niebezpieczeństwo wystąpienia incydentów w świecie cyfrowym oraz maksymalnie ograniczających ryzyko strat z nimi związanych[12]. Konieczne jest zapewnienie gwarancji bezpieczeństwa i poufności informacji na poziomie technicznym w cyberprzestrzeni. Kolejno, równie istotne jest zagwarantowanie nienaruszalności systemów teleinformatycznych poprzez zapewnienie i monitorowanie ich odporności na incydenty oraz zapewnienie stałej ich dostępności, a także przechowywanych i przetwarzanych w nich zasobów[13]. Działania te muszą obejmować nie tylko krytyczną infrastrukturę teleinformatyczną w sektorze publicznym, ale również sektor prywatny. Konieczna jest współpraca, wymiana informacji i doświadczeń pomiędzy poszczególnymi sektorami w zakresie monitorowania incydentów, sposobów reagowania na nie, określania ich przyczyn, prowadzenia analiz związanych z ich wystąpieniem, wyciągania wniosków i podejmowania działań na przyszłość w celu wyeliminowania ich ponownego wystąpienia[14].

W UE na gruncie prawa skutek ten ma zostać osiągnięty przez wprowadzone w 2016 r. prawodawstwo – stosowane od 25.5.2018 r. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[15] oraz dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[16], która miała zostać wdrożona przez państwa członkowskie UE do 9.5.2018 r. Przyjęcie wskazanych dwóch aktów prawnych stanowi wprost realizację strategii jednolitego rynku cyfrowego, której celem jest m.in. zwiększenie zaufania obywateli wspólnoty europejskiej względem usług cyfrowych i poprawa ich bezpieczeństwa[17]. Wspomnieć należy, że oprócz wskazanych aktów prawnych ramy i podstawy prawne zwalczania cyberprzestępczości tworzy dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z 12.8.2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW[18]. Dyrektywa NIS nakłada na państwa członkowskie UE obowiązek poszerzenia ich współpracy w kwestii zapewnienia cyberbezpieczeństwa oraz zwalczania cyberprzestępczości. Dyrektywa ta ustanawia nowe obowiązki dla państw członkowskich w zakresie opracowania, wdrożenia i stosowania strategii bezpieczeństwa sieci i systemów informatycznych, rozwijając współpracę w tym zakresie w ramach wspólnoty, oraz tworzy sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieć CSIRT)[19]. Wreszcie dyrektywa NIS wprowadza nowe standardy dotyczące odporności systemów informatycznych na ataki hakerskie w kluczowych sektorach gospodarki, w zakresie świadczenia usług kluczowych oraz usług cyfrowych, takich jak wyszukiwarki, przechowywanie danych w chmurze czy internetowe platformy handlowe[20].

Wpływ ustawy o krajowym systemie cyberbezpieczeństwa na działalność dostawców usług cyfrowych

Dnia 28.8.2018 r. weszła w życie ustawa implementująca do polskiego porządku prawnego dyrektywę NIS, czyli ustawa z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa[21] określająca organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy,

[9] *S. Kotecka*, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, Legalis/el. 2016.

[10] Tamże, Legalis el./2016. Zob. także: *K. Szczepanowska-Kozłowska*, *J. Ostrowska*, Poland Chapter 22, [w:] Global Legal Group, The International Comparative Legal Guide to: Cybersecurity 2018 1-st Edition, A practical cross-border insight into cybersecurity work, Global Legal Group 2018, s. 141 i n.

[11] *S. Kotecka*, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, Legalis/el. 2016.

[12] *T. Tołpa*, *J. Protasiewicz*, *M. Kozłowski*, *B. Bułkszas*, Zagrożenia, nadużycia i bezpieczeństwo w systemach informatycznych a granice ochrony praw podstawowych, Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne 2015, s. 542.

[13] *M.-T. Holzleitner*, *J. Reichl*, European provisions for cyber security in the smart grid – an overview of the NIS-directive, Springer Verlag Wien 2017.

[14] *S. Kotecka*, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, Legalis/el. 2016.

[15] Dz.Urz. UE L Nr 199, s. 1, dalej jako: RODO.

[16] Dz.Urz. UE L Nr 194, s. 1; dalej jako: dyrektywa NIS.

[17] *M. Olszewska*, Cyberbezpieczeństwo jako przedmiot analizy przestrzennej, Legalis/el.2018.

[18] Dz.Urz. UE L Nr 218, s. 8.

[19] Art. 1 ust. 2 dyrektywy NIS.

[20] *M. Siemaszkiewicz*, Internet rzeczy – wyzwania cyberbezpieczeństwa, Edukacja Prawnicza 2018, Nr 1, s. 51 i n.

[21] Dz.U. poz. 1560; dalej jako: KrajSysCybU.

a także wskazująca zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej[22]. Zasadniczym celem tej ustawy jest stworzenie krajowego systemu cyberbezpieczeństwa mającego zapewnić cyberbezpieczeństwo 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[23]. Kluczowe z punktu widzenia nowej regulacji pojęcie cyberbezpieczeństwa zostało zdefiniowane w art. 2 pkt 4 KrajSysCybU. W myśl tego przepisu cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Dostawcy usług cyfrowych objęci Krajowym Systemem Cyberbezpieczeństwa

Artykuł 4 KrajSysCybU zawiera wyliczenie podmiotów, które objęte zostały Krajowym Systemem Cyberbezpieczeństwa. Zgodnie z pkt 2 tego przepisu do tego systemu zalicza się także dostawców usług cyfrowych.

Warto zwrócić uwagę, że zgodnie z art. 1 ust. 2 KrajSysCybU jej przepisów nie stosuje się do przedsiębiorców telekomunikacyjnych[24] – w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, a także do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE[25], oraz podmiotów wykonujących działalność leczniczą tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

W rozumieniu art. 17 ust. 1 KrajSysCybU 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. Podobnie jak w dyrektywie NIS, w ustawie o krajowym systemie cyberbezpieczeństwa za dostawców usług cyfrowych, w myśl tego przepisu, nie są uważani mikroprzedsiębiorcy[26] i mali przedsiębiorcy[27]. Powodem wyłączenia tych podmiotów z kategorii dostawców usług cyfrowych może być fakt, że wymagane ustawą o krajowym systemie cyberbezpieczeństwa środki bezpieczeństwa oraz nałożone obowiązki mogą stanowić dla nich nieproporcjonalne obciążenie[28]. Kolejno wskazać należy, że w myśl art. 2 pkt 15 KrajSysCybU usługą cyfrową jest usługa świadczona drogą elektroniczną w rozumieniu przepisów ustawy z 18.7.2002 r. o świadczeniu usług drogą elektroniczną[29], wymieniona w załączniku Nr 2 do ustawy o krajowym systemie cyberbezpieczeństwa.

Analiza ww. załącznika Nr 2 oraz przepisów będących przedmiotem odesłania ustawowego pozwala na zdefiniowanie usługi cyfrowej jako usługi, która jest usługą internetowej platformy handlowej, usługą przetwarzania w chmurze lub usługą wyszukiwarki internetowej, i która świadczona jest bez jednoczesnej obecności stron (na odległość) poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej (w rozumieniu prawa telekomunikacyjnego), tj. za pomocą systemów transmisyjnych oraz urządzeń komutacyjnych lub przekierowujących, a także innych zasobów, w tym nieaktywnych elementów sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.

Przywołane w powyższej definicji kategorie usług cyfrowych zostały zdefiniowane ustawowo w załączniku Nr 2 do ustawy o krajowym systemie cyberbezpieczeństwa. Zgodnie z tym załącznikiem internetowa platforma handlowa to usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na

[22] Art. 1 ust. 1 KrajSysCybU.

[23] Art. 3 KrajSysCybU.

[24] O których mowa w ustawie z 16.7.2004 r. – Prawo telekomunikacyjne, t.j. Dz.U. z 2018 r. poz. 1954 ze zm.

[25] Dz.Urz. UE L Nr 257, s. 73; dalej jako: rozporządzenie eIDAS. Usługi zaufania to zgodnie z art. 3 pkt 16 rozporządzenie eIDAS usługi elektroniczne zazwyczaj świadczone za wynagrodzeniem i obejmujące: a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

[26] W myśl art. 7 ust. 1 pkt 1 ustawy z 6.3.2018 r. – Prawo przedsiębiorców (Dz.U. poz. 646 ze zm.; dalej jako: PrPrzedsU) mikroprzedsiębiorcy to przedsiębiorcy, którzy w co najmniej jednym roku z dwóch ostatnich lat obrotowych zatrudniali średniorocznie mniej niż 10 pracowników oraz osiągnęli roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 2 mln euro, lub sumy aktywów ich bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 2 mln euro.

[27] Zgodnie z art. 7 ust. 1 pkt 2 PrPrzedsU mali przedsiębiorcy to przedsiębiorcy, którzy w co najmniej jednym roku z dwóch ostatnich lat obrotowych zatrudniali średniorocznie mniej niż 50 pracowników oraz osiągnęli roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 10 mln euro, lub sumy aktywów ich bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 10 mln euro, i którzy nie są mikroprzedsiębiorcami.

[28] *M.-T. Holzleitner, J. Reichl*, European provisions for cyber security in the smart grid – an overview of the NIS-directive, Springer Verlag Wien 2017.

[29] Dz.U. z 2017 r. poz. 1219 ze zm.

stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy korzystającej z usług świadczonych przez internetową platformę handlową. Usługę przetwarzania w chmurze ustawodawca zdefiniował jako usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników, natomiast wyszukiwarka internetowa to usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiająca w wyniku odnośniki odnoszące się do informacji związanych z zapytaniem.

Należy zauważyć, że przytoczona powyżej ustawowa definicja internetowej platformy handlowej jest stosunkowo nieostra i jej interpretacja w praktyce może budzić zasadnicze wątpliwości. W celu jej uzupełnienia należy sięgnąć posiłkowo do treści motywu 15 preambuły dyrektywy NIS, zgodnie z którym internetowa platforma handlowa umożliwia konsumentom i przedsiębiorcom handlowym zawieranie umów sprzedaży lub umów o świadczenie usług online z przedsiębiorcami handlowymi i jest ostatecznym miejscem zawierania tych umów. W przypadku gdy możliwe jest ostateczne zawarcie umowy, nie powinna ona obejmować usług online, które spełniają wyłącznie funkcję pośredniczącą wobec usług stron trzecich. Nie powinna zatem obejmować usług online, które porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego w celu zakupu produktu. W opinii autorki, w kontekście treści motywu 15 dyrektywy 2016/1148, a także z uwagi na *ratio legis* analizowanej regulacji, należy również uznać, że działalność przedsiębiorców handlowych pośredniczących w sprzedaży towarów i świadczeniu usług za pośrednictwem własnej internetowej platformy handlowej, która jest ostatecznym miejscem zawierania umów, we wskazanym zakresie zawiera się w istocie rzeczy w definicji usługi cyfrowej internetowej platformy handlowej.

Jak rozumieć definicję usługi przetwarzania w chmurze? Po pierwsze, posiłkując się motywem 17 dyrektywy NIS, można przyjąć, że zakres pojęcia „zasoby obliczeniowe" obejmuje sieci, serwery lub inną infrastrukturę, pamięć, aplikacje i usługi. Zgodnie z tym motywem pojęcie „skalowalne" odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuacje zapotrzebowania. Natomiast pojęcie „elastyczny zbiór" charakteryzuje zasoby obliczeniowe, które są przydzielane i uwalniane zależnie do zapotrzebowania, aby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia. „Wspólne wykorzystywanie przez wielu użytkowników" polega natomiast na dzieleniu przez wielu użytkowników wspólnego dostępu do usługi, jednak przetwarzanie w ramach tej usługi odbywa się oddzielnie dla każdego z użytkowników, przy jednoczesnym świadczeniu usługi z tego samego sprzętu elektronicznego.

Jak z kolei wskazano w motywie 16, definicja wyszukiwarki internetowej nie powinna obejmować funkcji wyszukiwania, które ograniczają się do treści na konkretnej stronie internetowej, bez względu na to, czy funkcja wyszukiwania jest zapewniana przez wyszukiwarkę zewnętrzną. Co więcej, podobnie jak w przypadku definicji internetowej platformy handlowej, tak również w zakresie definicji wyszukiwarki internetowej nie powinny znajdować się usługi online, które porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego, aby tam dokonał zakupu produktu.

Obowiązki dostawców usług cyfrowych

Wskazać należy więc, że zgodnie z art. 17 ust. 2 zd. 1 KrajSysCybU dostawca usługi cyfrowej jest obowiązany podejmować właściwe i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki zarządzania ryzykiem zostały określone w rozporządzeniu wykonawczym Komisji (UE) 2018/151 z 30.1.2018 r. ustanawiającym zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi rodzajami ryzyka dla bezpieczeństwa sieci i systemów informatycznych oraz parametrów służących do określenia, czy incydent ma istotny wpływ[30]. W rozporządzeniu tym doprecyzowane zostały również elementy, jakie mają zostać uwzględnione przez dostawców usług cyfrowych przy określaniu i przedsiębraniu środków mających na celu zapewnienie poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez nich w kontekście oferowania usług cyfrowych, jak również parametry, które należy wziąć pod uwagę w celu ustalenia, czy incydent ma istotny wpływ na świadczenie tych usług.

W myśl art. 17 ust. 2 zd. 2 KrajSysCybU środki zarządzania ryzykiem, a więc skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka[31] zapewniają cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniają 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

[30] Dz.Urz. UE L Nr 26, s. 48; dalej jako: rozporządzenie Nr 2018/151.
[31] Art. 2 pkt 19 KrajSysCybU.

z normami, międzynarodowymi, o których mowa w rozporządzeniu Nr 2018/151.

1. Bezpieczeństwo systemów informacyjnych i obiektów

W myśl art. 2 ust. 1 rozporządzenia Nr 2018/151 bezpieczeństwo sieci i systemów informatycznych oraz ich środowiska fizycznego obejmuje następujące elementy:

- systematyczne zarządzanie sieciami i systemami informatycznymi, co oznacza mapowanie systemów informatycznych oraz ustanowienie zestawu odpowiednich polityk w zakresie zarządzania bezpieczeństwem informacji, w tym analiz ryzyka, zasobów ludzkich, bezpieczeństwa operacji, architektury bezpieczeństwa, zabezpieczenia danych i zarządzania cyklem życia systemu oraz, w stosownych przypadkach, szyfrowania i zarządzania nim;
- bezpieczeństwo fizyczne i środowiskowe, które oznacza dostępność zestawu środków mających na celu ochronę bezpieczeństwa sieci i systemów informatycznych dostawców usług cyfrowych przed szkodami z zastosowaniem całościowego podejścia do kwestii zagrożeń opartego na analizie ryzyka, które uwzględnia np. awarie systemu, błędy ludzkie, działania złośliwe bądź zjawiska naturalne;
- bezpieczeństwo dostaw oznacza ustanowienie oraz utrzymywanie odpowiednich polityk w celu zagwarantowania dostępności oraz, w stosownych przypadkach, identyfikowalności krytycznych dostaw wykorzystywanych do świadczenia usług;
- kontrole dostępu do sieci i systemów informatycznych, co oznacza dostępność zestawu środków, które mają zagwarantować, że dostęp fizyczny i dostęp logiczny do sieci i systemów informatycznych, w tym administracyjne bezpieczeństwo sieci i systemów informatycznych, są uprawnione i ograniczone w oparciu na wymogi dotyczące prowadzenia działalności i bezpieczeństwa.

2. Postępowanie w przypadku obsługi incydentu

Zgodnie z art. 2 ust. pkt 10 KrajSysCybU obsługa incydentu to czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu. W odniesieniu do postępowania w przypadku incydentu środki przedsiębrane przez dostawcę usług cyfrowych, zgodnie z art. 2 ust. 2 rozporządzenia Nr 2018/151, obejmują:

- utrzymywanie i testowanie procesów oraz procedur wykrywania w celu zapewnienia terminowej i odpowiedniej wiedzy na temat nietypowych zdarzeń;
- procesy i polityki dotyczące zgłaszania incydentów oraz identyfikowania niedociągnięć i słabych punktów w jego systemach informatycznych;
- reagowanie zgodnie z ustanowionymi procedurami oraz składanie sprawozdań z wyników przedsięwziętych środków;
- ocenę powagi danego incydentu, dokumentowanie wiedzy uzyskanej z analizy incydentów oraz gromadzenie odpowiednich informacji, które mogą stanowić dowody i wspierać proces ciągłego doskonalenia.

3. Zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej

Zarządzanie ciągłością działania, w myśl art. 2 ust. 3 rozporządzenia wykonawczego 2018/151, oznacza zdolność do utrzymania lub, w razie potrzeby, przywrócenia realizacji usług na uprzednio określonych dopuszczalnych poziomach, po wystąpieniu zakłócenia, i obejmuje:

- ustanowienie i stosowanie planów awaryjnych w oparciu o analizę wpływu na działalność w celu zapewnienia ciągłości usług świadczonych przez dostawców usług cyfrowych, co jest oceniane i testowane w regularnych odstępach czasu, np. przez ćwiczenia;
- zdolności w zakresie przywracania gotowości do pracy po katastrofie, które są oceniane i testowane w regularnych odstępach czasu, na przykład przez ćwiczenia.

4. Monitorowanie, audyt i testowanie

Monitorowanie, audyt i testowanie, w myśl art. 2 ust. 4 rozporządzenia wykonawczego 2018/151, obejmują ustanowienie i utrzymywanie polityk w zakresie:

- przeprowadzania zaplanowanej sekwencji obserwacji lub pomiarów w celu dokonania oceny, czy sieci i systemy informatyczne działają zgodnie z zamierzeniem;
- inspekcji i weryfikacji mających na celu sprawdzenie, czy stosuje się normę lub zbiór wytycznych, czy rejestry są dokładne, a także czy realizowane są cele w zakresie efektywności i skuteczności;
- procesu mającego na celu ujawnienie wad mechanizmów bezpieczeństwa sieci i systemów informatycznych, które służą ochronie danych i utrzymaniu funkcjonalności zgodnie z zamierzeniem. Tego rodzaju proces obejmuje procesy techniczne i personel zaangażowany w przepływ operacji.

5. Najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi

Normy międzynarodowe, zgodnie z art. 2 ust. 5 rozporządzenia Nr 2018/151, oznaczają normy przyjęte przez międzynarodową jednostkę normalizacyjną, o której mowa w art. 2 ust. 1 lit. a) rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 1025/2012, tj. Międzynarodową Organizację Normalizacyjną (ISO), Międzynarodową Komisję Elektrotechniczną (IEC) i Międzynarodowy Związek Telekomunikacyjny (ITU). Stosowane mogą być również europejskie lub uznane

międzynarodowe normy i specyfikacje mające znaczenie dla bezpieczeństwa sieci i systemów informatycznych, w tym istniejące normy krajowe.

6. Środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową

W myśl art. 17 ust. 3 KrajSysCybU dostawca usługi cyfrowej podejmuje ponadto środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi. Ciągłość ta może mieć wpływ na kluczową działalność gospodarczą i społeczną w UE, wszak zakłócenie usług cyfrowych mogłoby uniemożliwić świadczenie innych usług, które są od nich zależne[32]. W dzisiejszych czasach, gdy z usług cyfrowych korzystają niemal wszyscy przedsiębiorcy, przerwanie ciągłości świadczenia takich usług mogłoby znacząco utrudnić funkcjonowanie takich przedsiębiorców, a także, co również podkreślono w motywie 48 preambuł dyrektywy NIS, znacząco wpłynąć na ich uczestnictwo w rynku wewnętrznym i handlu transgranicznym w Unii.

Pozostałe obowiązki związane z wystąpieniem incydentów w cyberprzestrzeni oraz ich odmienność w zależności od rodzajów incydentów

Należy zauważyć, że na gruncie przepisów ustawy o krajowym systemie cyberbezpieczeństwa szczególną rolę odgrywają obowiązki dostawców usług cyfrowych dotyczące reakcji na wystąpienie incydentów. W pierwszej kolejności należy wskazać, że zgodnie z art. 18 ust. 1 pkt 1 KrajSysCybU, dostawca usługi cyfrowej przeprowadza czynności umożliwiające wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów.

W rozumieniu art. 2 pkt 5 KrajSysCybU incydentem jest zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Ustawa o krajowym systemie cyberbezpieczeństwa definiuje także szczególne kategorie incydentów, które mogą mieć niekorzystny wpływ na odporność systemów informacyjnych dostawców usług cyfrowych.

Po pierwsze, wyróżnia się incydent istotny, czyli taki, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia Nr 2018/151[33]. Zgodnie z tym przepisem dany incydent uznaje się za mający istotny wpływ, jeżeli zaistniała co najmniej jedna z wymienionych w nim przesłanek. Będziemy mieć zatem do czynienia z incydentem istotnym, gdy usługa świadczona przez dostawcę usług cyfrowych była niedostępna przez ponad 5 000 000 użytkownikogodzin[34] bądź też gdy incydent doprowadził do utraty integralności, autentyczności lub poufności przechowywanych lub przekazywanych bądź przetwarzanych danych lub powiązanych usług, oferowanych bądź dostępnych poprzez sieci i systemy informatyczne dostawcy usług cyfrowych, która dotknęła ponad 100 000 użytkowników w UE. Incydent istotny nastąpi także wtedy, gdy spowoduje ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych lub gdy wyrządził co najmniej jednemu użytkownikowi w UE stratę materialną, której wysokość przekracza 1 000 000 euro.

Po drugie, ustawa wprowadza również kategorię incydentu krytycznego. Jest to incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT GOV, CSIRT MON, CSIRT NASK[35].

Wreszcie na gruncie analizowanej regulacji wyróżnić można również kategorię incydentów zwykłych, tj. takich zdarzeń, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo, ale nie są ani incydentami krytycznymi, ani incydentami istotnymi.

Szczególną uwagę zwrócić należy na dodatkowe obowiązki przedsiębiorców związane z wystąpieniem incydentów istotnych i incydentów krytycznych. Stąd odróżnić należy dwa rodzaje postępowania w przypadku wystąpienia incydentów, w zależności od tego, czy zachodzi incydent zwykły, czy też incydent istotny lub krytyczny. Dopiero bowiem sklasyfikowanie incydentu jako incydentu istotnego czy też krytycznego pociąga za sobą odmienności w zakresie postępowania z nim w postaci dodatkowych obowiązków omówionych w dalszej części rozważań.

W myśl art. 18 ust. 2 KrajSysCybU w celu sklasyfikowania incydentu jako istotnego dostawca usługi cyfrowej uwzględnia w szczególności liczbę 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. Dostawca usługi cyfrowej, zgodnie z art. 18 ust. 3 KrajSysCybU, klasyfikując incydent jako istotny, ocenia istotność wpływu incydentu na świadczenie usługi cyfrowej na podstawie parametrów, o których mowa powyżej, oraz progów określonych w rozporządzeniu wykonawczym 2018/151.

[32] Motyw 48 preambuły dyrektywy NIS.

[33] Art. 1 pkt 7 KrajSysCybU.

[34] Pojęcie „użytkownikogodziny" odnosi się do liczby dotkniętych incydentem użytkowników w Unii przez okres sześćdziesięciu minut

[35] Art. 1 pkt 6 KrajSysCybU.

Tab. 1. Parametry i odpowiednie progi, jakie należy wziąć pod uwagę w celu określenia, czy wpływ incydentu jest istotny

Parametr	Progi
Liczba użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług	Dostawca usług cyfrowych musi być w stanie oszacować jedną z następujących liczb: 1) liczba dotkniętych incydentem osób fizycznych i osób prawnych, z którymi zawarto umowę na świadczenie danej usługi, lub 2) liczba dotkniętych incydentem użytkowników, którzy korzystali z tej usługi, na podstawie w szczególności wcześniejszych danych o ruchu.
Czas trwania incydentu	Dostawca usług cyfrowych musi ustalić okres, jaki upływa od zakłócenia właściwego świadczenia usługi pod względem jej dostępności, autentyczności, integralności lub poufności, do czasu przywrócenia stanu normalnego.
Zasięg geograficzny obszaru, którego dotyczy incydent	Dostawca usług cyfrowych musi być w stanie ustalić, czy dany incydent ma wpływ na świadczenie jego usług w poszczególnych państwach członkowskich.
Zakres zakłócenia funkcjonowania usługi	Zakres ten dostawca usług cyfrowych powinien mierzyć w odniesieniu do jednego lub większej liczby następujących aspektów osłabionych w wyniku danego incydentu: dostępność, autentyczność, integralność lub poufność danych lub powiązanych usług.
Zakres wpływu incydentu na działalność gospodarczą i społeczną	Dostawca usług cyfrowych musi być w stanie – w oparciu na wskazówki, takie jak charakter jego stosunków umownych z klientem lub, w stosownych przypadkach, potencjalna liczba użytkowników dotkniętych incydentem – stwierdzić, czy incydent spowodował znaczne straty materialne bądź niematerialne dla użytkowników, na przykład odnośnie do zdrowia, bezpieczeństwa lub uszkodzenia mienia.

W przypadku gdy analiza powyższych parametrów pozwoli na ustalenie, iż dany incydent nie spełnia przesłanek uznania go za incydent istotny, uznać należy, że zaistniałe zdarzenie ma charakter incydentu zwykłego i konsekwentnie nie rodzi ono po stronie dostawcy usługi cyfrowej żadnych obowiązków ponad te, jakie wynikają z przedstawionej powyżej definicji obsługi incydentu. Powyższe oznacza, że w sytuacji uznania zdarzenia za incydent zwykły dostawca usług cyfrowych obowiązany będzie wyłącznie dokonać priorytetyzacji, a także podjąć działania naprawcze i ograniczyć skutki incydentu zgodnie z procedurami, które wdrożył, realizując obowiązek, o którym mowa w art. 17 ust. 2 pkt 2 oraz art. 17 ust. 3 KrajSysCybU.

Szczególne obowiązki dostawców usług cyfrowych związane z kategorią incydentów istotnych i incydentów krytycznych

Zgodnie z art. 18 KrajSysCybU dostawca usługi cyfrowej klasyfikując incydent jako istotny jest obowiązany zgłosić go niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego organu, tj. CSIRT GOV, CSIRT MON lub CSIRT NASK. Zgłoszenie, o którym mowa powyżej, jest przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji[36]. Informacje, które przedsiębiorca musi zawrzeć w zgłoszeniu, wskazano w art. 19 ust. 1 KrajSysCybU. Zgłaszając incydent, należy przede wszystkim opisać przyczynę i źródło incydentu, jego wpływ na świadczenie usługi cyfrowej, w tym liczbę użytkowników, których dotknął, czas trwania incydentu, jego zasięg geograficzny, zakres zakłócenia funkcjonowania usługi cyfrowej oraz zakres wpływu incydentu na działalność gospodarczą i społeczną. Oprócz tego przedsiębiorca ma obowiązek przedstawić w zgłoszeniu informacje umożliwiające właściwemu CSIRT określenie, czy incydent istotny dotyczy dwóch lub większej liczby państw członkowskich UE. Wreszcie należy także przedstawić podjęte działania zapobiegawcze i naprawcze.

Należy podkreślić, że dostawca usługi cyfrowej obowiązany jest przekazać informacje znane mu w chwili dokonywania zgłoszenia. Informacje te dostawca usług cyfrowych uzupełnia następnie w trakcie obsługi incydentu istotnego[37]. Co ważne, jak wynika z brzmienia art. 19 ust. 3 KrajSysCybU, obowiązek przekazania w niezbędnym zakresie informacji stanowiących tajemnice prawnie chronione, w tym stanowiących tajemnicę przedsiębiorstwa, powstaje, wyłącznie gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. Właściwy CSIRT może zwrócić się do dostawcy usługi cyfrowej o uzupełnienie zgło-

[36] Art. 18 ust. 5 KrajSysCybU.
[37] Art. 19 ust. 2 KrajSysCybU.

szenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań ustawowych. Należy pamiętać, że informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, dostawcy usług cyfrowych mają obowiązek odpowiednio oznaczyć w zgłoszeniu[38].

Podkreślenia wymaga fakt, że zgodnie z brzmieniem art. 18 ust. 4 KrajSysCybU dostawca usługi cyfrowej nie ma obowiązku dokonania zgłoszenia, o którym mowa wyżej, gdy nie posiada informacji pozwalających na ocenę istotności wpływu incydentu na świadczenie usługi cyfrowej. Powyższe oznacza, że w braku możliwości oceny istotności wpływu incydentu na świadczenie usługi cyfrowej incydent będzie obsługiwany tak jak incydent zwykły.

Zgodnie z art. 18 ust. 1 pkt 5 KrajSysCybU dostawca usług cyfrowych zapewnia obsługę incydentu istotnego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe.

Na dostawcy usługi cyfrowej spoczywa również obowiązek usunięcia, w wyznaczonym terminie, podatności, czyli właściwości systemu informacyjnego, które mogą być wykorzystane przez zagrożenie cyberbezpieczeństwa, tj. przez potencjalną przyczynę wystąpienia incydentu[39], a które doprowadziły lub mogłyby doprowadzić do incydentu istotnego, na wezwanie organu właściwego do spraw cyberbezpieczeństwa, jeśli z wnioskiem o takie wezwanie w trakcie koordynacji obsługi incydentu istotnego wystąpi CSIRT MON, CSIRT NASK lub CSIRT GOV[40]. W przypadku uznania zgłoszonego incydentu istotnego za incydent krytyczny przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV dostawca usług cyfrowych jest obowiązany ponadto zapewnić w niezbędnym zakresie dostęp do informacji dla właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV o incydentach zakwalifikowanych jako krytyczne[41]. Co więcej, w myśl art. 18 ust. 1 pkt 7 KrajSysCybU dostawca usługi cyfrowej przekazuje operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora. Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy (m.in. przewoźnicy lotniczy, przedsiębiorstwa energetyczne, banki krajowe, podmioty lecznicze), posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej[42]. Należy wskazać również, że usługą kluczową jest usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych[43], tj. m.in. transport lotniczy pasażerski, udzielanie opieki zdrowotnej.

Warto ponadto zwrócić uwagę na możliwość dobrowolnego przekazywania właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV informacji nieobjętych ustawowym obowiązkiem informacyjnym. W myśl art. 20 KrajSysCybU dostawca usługi cyfrowej może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV również informacje o incydentach innych niż istotne (tj. o incydentach zwykłych), a także o zagrożeniach cyberbezpieczeństwa, szacowaniu ryzyka, podatnościach oraz wykorzystywanych technologiach. Informacje te są przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania ich w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Kary za niedopełnienie obowiązków

Należy podkreślić, że w przepisach ustawy o krajowym systemie cyberbezpieczeństwa przewidziane zostały kary pieniężne, nakładane w drodze decyzji organu właściwego do spraw cyberbezpieczeństwa za naruszenie przez dostawcę usług cyfrowych ustawowo określonych obowiązków. W przypadku gdy dostawca usług cyfrowych nie wykonuje obowiązku zgłoszenia incydentu istotnego, podlega karze pieniężnej do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego[44]. Jeżeli dostawca usług cyfrowych nie wykonuje obowiązku obsługi incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, m.in. obowiązku przekazania niezbędnych danych, w tym danych osobowych, podlega karze pieniężnej do 20 000 zł[45]. Ponadto gdy dostawca usług cyfrowych nie usuwa w wyznaczonym terminie podatności, które doprowadziły lub mogłyby doprowadzić do incydentu istotnego, na wezwanie organu właściwego do spraw cyberbezpieczeństwa, jeśli z wnioskiem o takie wezwanie w trakcie koordynacji obsługi incydentu istotnego wystąpi CSIRT MON, CSIRT NASK lub CSIRT GOV, podlega karze pieniężnej do 20 000 zł[46]. Co istotne, kary, o których mowa powyżej, mogą zostać nałożone, również w przypadku gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli organ właściwy do spraw cyberbezpieczeństwa uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia[47].

Jakkolwiek określone powyżej przypadki naruszeń stanowią katalog zamknięty, a konsekwentnie niedopełnienie innych obowiązków niż wskazane powyżej co do zasady nie

[38] Art. 19 ust. 4 i 5 KrajSysCybU.
[39] Art. 2 pkt 11 i 17 KrajSysCybU.
[40] Art. 18 ust. 1 pkt 6 KrajSysCybU.
[41] Art. 18 ust. 1 pkt 2 KrajSysCybU.
[42] Art. 5 ust. 1 KrajSysCybU.
[43] Art. 2 pkt 16 KrajSysCybU.
[44] Art. 73 ust. 2 pkt 1 w zw. z art. 73 ust. 3 pkt 12 KrajSysCybU.
[45] Art. 73 ust. 2 pkt 2 w zw. z art. 73 ust. 3 pkt 13 KrajSysCybU.
[46] Art. 73 ust. 2 pkt 3 w zw. z art. 73 ust. 3 pkt 13 KrajSysCybU.
[47] Art. 76 KrajSysCybU.

pociąga za sobą odpowiedzialności finansowej, w przepisach ustawy o krajowym systemie cyberbezpieczeństwa przewidziana została wyjątkowa odpowiedzialność uzależniona od czasu trwania naruszenia i jego skutków. Należy bowiem podkreślić, że jeśli w wyniku kontroli organ właściwy do spraw cyberbezpieczeństwa stwierdzi, że operator usługi kluczowej albo dostawca usługi cyfrowej uporczywie narusza przepisy ustawy, powodując: 1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi; 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych – organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 1 000 000 zł[48]. Literalne brzmienie powyższego przepisu (możliwość jego zastosowania w wypadku „uporczywego naruszenia przepisów ustawy") uzasadnia pogląd, że dotyczy on naruszenia jakichkolwiek przepisów, jeśli naruszenie to jest uporczywe i wypełnia chociażby jedną z przesłanek wskazanych w pkt 1 lub 2 powyżej.

Podsumowanie

Analiza przepisów ustawy o krajowym systemie cyberbezpieczeństwa implementującej dyrektywę NIS prowadzi do wniosku, że wiele podmiotów sektora prywatnego spełnia przesłanki kwalifikujące ich uznanie za dostawcę usług cyfrowych w rozumieniu przepisów ustawy. Konstatacja ta pociąga za sobą konsekwencje w postaci objęcia tej kategorii dostawców usług cyfrowych krajowym systemem cyberbezpieczeństwa i nałożenia nań obowiązków w zakresie zarządzania ryzykiem, zapobiegania i minimalizacji wpływu incydentów na usługę cyfrową, a także ich obsługi. Pamiętać należy, że celem regulacji ustawowej jest wypracowanie niezbędnych reguł postępowania w celu lepszego zapewnienia cyberbezpieczeństwa, a przez to zapewnienie ciągłości świadczenia usług cyfrowych. Nawet jeśli usługi cyfrowe świadczone przez dostawców sektora prywatnego nie są usługami podstawowymi dla ogółu ludności, zapewnienie ich ciągłości może mieć wpływ na kluczową działalność gospodarczą i społeczną nie tylko konkretnego kraju UE, ale także całej wspólnoty. Nie może umknąć uwadze, że zakłócenie usług cyfrowych mogłoby uniemożliwić świadczenie innych usług, które są od nich zależne, a które to mogą być usługami podstawowymi dla gospodarki i społeczeństwa UE. W porównaniu do RODO, którego głównym celem jest ochrona danych osobowych podmiotów prywatnych, ustawa o krajowym systemie cyberbezpieczeństwa kładzie główny nacisk na zapewnienie bezpieczeństwa sieci i systemów teleinformatycznych. W akcie tym ustawodawca stosuje wiele podobnych mechanizmów związanych z identyfikowaniem, szacowaniem i zarządzaniem ryzykiem oraz powiela znaczną część obowiązków określonych w RODO. Istotna różnica dotyczy wyłączenia w ustawie o krajowym systemie cyberbezpieczeństwa mikroprzedsiębiorców i małych przedsiębiorców z konieczności stosowania środków bezpieczeństwa i realizacji obowiązków tam określonych. Fakt ten może wynikać z nieproporcjonalności obowiązków i związanych z nimi nierozerwalnie ciężarów, które to byłyby za wysokie w odniesieniu do wielkości tych przedsiębiorców. Trudno zatem stwierdzić, że nałożone obowiązki będą wysoce uciążliwe dla określonej w ustawie o krajowym systemie cyberbezpieczeństwa kategorii dostawców usług cyfrowych.

[48] Art. 73 ust. 5 KrajSysCybU.

Słowa kluczowe: cyberbezpieczeństwo, dostawcy usług cyfrowych, krajowy system cyberbezpieczeństwa, obowiązki dostawców usług cyfrowych

Obligations of digital service providers under the act on the national cybersecurity system as an element of improvement of security in the digital world and prevention of cybercrime

The aim of the present study is to systematize and analyze the obligations of digital service providers under the national cybersecurity system. The study also focuses on identifying which entities are considered as providers of digital services within the meaning of this act. The analysis of the obligations refers to the relevant provisions of EU law. The author also pays attention to the differences in the scope of obligations necessary to perform which are related to the occurrence of events that may have a negative impact on cybersecurity connected with qualifications of such incidents as significant or critical and to penalties that may result from the failure of digital service providers to fulfil their obligations under the act.

Keywords: cybersecurity, digital service providers, national cybersecurity system, obligations of digital service providers.