Tomasz Proć*

Odpowiedzialność dostawcy usług cyfrowych w Krajowym Systemie Cyberbezpieczeństwa

Spis treści

Streszczenie

W artykule autor przedstawia zagadnienie odpowiedzialności dostawców usług cyfrowych za naruszenie zasad cyberbezpieczeństwa. Omówione zostały obowiązki dostawców usług cyfrowych wynikające z przepisów ustawy o krajowym systemie cyberbezpieczeństwa w kontekście ochrony użytkowników oraz sankcje, jakie grożą dostawcom usług cyfrowych na gruncie tej regulacji. Poruszona została kwestia ochrony użytkowników usług cyfrowych z perspektywy przepisów ochrony danych osobowych oraz sankcje wynikające z tych regulacji. Autor analizuje również szczególną odpowiedzialność dostawców usług cyfrowych względem konsumentów.

Słowa kluczowe: cyberbezpieczeństwo; użytkownik; dostawca usług cyfrowych; techniczne i organizacyjne środki bezpieczeństwa; dane osobowe.

JEL: K23, K24

I. Wprowadzenie

Na obecnym etapie rozwoju sektora usług elektronicznych, zapewnienie cyberbezpieczeństwa stanowi jeden z podstawowych elementów budowania zaufania do cyfrowej struktury gospodarki oraz usług publicznych. Dostawcy usług cyfrowych nie zawsze przywiązują do tego zagadnienia należyta wagę i nawet presja ze strony użytkowników nie zawsze prowadzi do wymiernych efektów w postaci zwiększonego poziomu cyberbezpieczeństwa (Rojszczak, 2018, s. 304). Regulacje na

* Autor jest radcą prawnym oraz Zastępcą Dyrektora w Departamencie Telekomunikacji w Ministerstwie Cyfryzacji.

poziomie unijnym (przede wszystkim dyrektywa NIS[1]) oraz w Polsce (przede wszystkim uksc[2]) nakładają na dostawców usług cyfrowych obowiązki związane z zapewnieniem cyberbezpieczeństwa na etapach zarówno analizy ryzyka (zapobieganie incydentom), jak i raportowania już zaistniałych incydentów.

Działalność obejmująca zapobieganie incydentom jest szczególnie istotna z punktu widzenia użytkowników. W najlepiej pojmowanym interesie użytkowników dostawcy usług cyfrowych powinni podejmować odpowiednie działania zapobiegawcze, zanim dojdzie do incydentu cyberbezpieczeństwa.

Ustawodawca nałożył na dostawców usług cyfrowych obowiązki związane z wdrożeniem odpowiednich środków bezpieczeństwa. Skuteczna egzekucja przedmiotowych obowiązków przez właściwe organy przyczyni się do ich pełnego wdrożenia. W szczególności głębszych rozważań wymaga ustalenie, jakie sankcje grożą dostawcom usług cyfrowych za naruszenie zasad cyberbezpieczeństwa wskazanych w UKSC.

W zakresie zapobiegania incydentom oraz w zakresie obowiązku stosowania odpowiednich środków bezpieczeństwa system cyberbezpieczeństwa znajduje wiele punktów stycznych z przepisami ochrony danych osobowych, które nakazują stosowanie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa. Ustalenie możliwej podstawy prawnej odpowiedzialności dostawcy usług cyfrowych w związku z niedopełnieniem obowiązku zapewnienia właściwego poziomu cyberbezpieczeństwa (w tym niewynikającego z UKSC) doprowadzi do wzrostu świadomości dostawców za nierealizowanie ustawowych obowiązków.

II. Użytkownik usług cyfrowych

Usługi cyfrowe są to usługi świadczone drogą elektroniczną wskazane w załączniku nr 2 do uksc, czyli:

1) internetowa platforma handlowa,
2) usługa przetwarzania w chmurze oraz
3) wyszukiwarka internetowa.

Katalog ten odpowiada katalogowi usług cyfrowych zdefiniowanemu w dyrektywie NIS. Usługa przetwarzania w chmurze oznacza usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników.

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, przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem. Warto zwrócić uwagę, że zgodnie z motywem (16) dyrektywy NIS 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. Nie powinna również obejmować usług online, które porównują cenę poszczególnych produktów lub usług

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L Nr 194, s. 1); dalej: dyrektywa NIS.

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (DzU 2018, poz. 1560 ze zm.); dalej: ustawa o krajowym systemie cyberbezpieczeństwa lub uksc.

różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego, aby tam dokonał zakupu produktu.

Z kolei internetowa platforma handlowa jest to usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową. W doktrynie zwrócono uwagę, że definicja ta może rodzić problemy interpretacyjne (Kruk, 2019). Aby ją prawidłowo zinterpretować należy wskazać na motyw (15) dyrektywy NIS, który wskazuje, że 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. Ponadto, dyrektywa NIS wskazuje, że sklepy z aplikacjami, które działają jako sklepy internetowe, umożliwiające cyfrową dystrybucję aplikacji lub oprogramowania stron trzecich, należy traktować jako rodzaj internetowej platformy handlowej. Interpretacja pojęcia „usług cyfrowych" zgodnie z uwzględnieniem postanowień motywów dyrektywy NIS wyraźnie ogranicza kategorie podmiotów prowadzących działalność w świecie cyfrowym regulowane w uksc.

Zgodnie z art. 17 uksc dostawcą usług cyfrowych może być 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, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców[3].

W uksc pojęcie „użytkownika" nie jest bezpośrednio zdefiniowane. Najczęściej używane jest ono w opisie kryteriów oceny incydentu mającego wpływ na cyberbezpieczeństwo[4]. Ustawa o krajowym systemie cyberbezpieczeństwa, jak również dyrektywa NIS nie wskazują wprost katalogu podmiotów, które mogą być użytkownikami. Analiza kategorii usług objętych definicją usług cyfrowych wskazuje, że katalog podmiotów, które mogą być użytkownikami może być bardzo szeroki i obejmować m.in. osoby fizyczne będące konsumentami, osoby fizyczne korzystające z usług cyfrowych w związku z prowadzoną działalnością gospodarczą, jak również inne niż osoby fizyczne, podmioty, w tym osoby prawne prowadzące działalność gospodarczą lub jej nieprowadzące oraz organy administracji państwowej. Katalog użytkowników usług cyfrowych jest bardzo szeroki i może zmieniać się wraz ze zmieniającymi się przepisami. Podsumowując, użytkownika usług cyfrowych należy rozumieć jako każdy podmiot (w tym osobę fizyczną) korzystający z usług cyfrowych.

[3] Mikroprzedsiębiorcy i mali przedsiębiorcy, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6.03.2018 – Prawo przedsiębiorców (DzU poz. 646 i 1479).

[4] Por. art. 6 pkt 2 uksc, art. 11 ust. 4 pkt 1 uksc i akty wykonawcze wydane na ich podstawie, art. 12 ust. 4 pkt 1 uksc.

III. Obowiązki dostawcy usług cyfrowych względem użytkownika

Regulacje cyberbezpieczeństwa nakładają na dostawców usług cyfrowych szereg obowiązków. Obowiązki można podzielić na dwie kategorie:

1) związane z zapewnieniem odpowiedniego poziomu cyberbezpieczeństwa;
2) związane z zaistnieniem incydentu.

Obydwie kategorie obowiązków, pomimo ich rozłącznego charakteru wynikającego z istoty obowiązków, są z sobą bezpośrednio powiązane: z jednej strony, niewypełnienie obowiązków związanych z zapewnieniem odpowiedniego poziomu cyberbezpieczeństwa zwiększa prawdopodobieństwo (ryzyko) wystąpienia incydentu, z drugiej – wystąpienie incydentu implikuje wątpliwości czy dostawca usług cyfrowych prawidłowo zapewnił odpowiedni poziom cyberbezpieczeństwa.

Do obowiązków związanych z zapewnieniem odpowiedniego poziomu cyberbezpieczeństwa należy zaliczyć w szczególności obowiązki wskazane w art. 17 ust. 2 uksc, tj. podejmowanie właściwych i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te powinny uwzględniać:

1) bezpieczeństwo systemów informacyjnych i obiektów;
2) postępowanie w przypadku obsługi incydentu;
3) zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej;
4) monitorowanie, audyt i testowanie;
5) najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2018/151.

Katalog środków technicznych i organizacyjnych został doprecyzowany w rozporządzeniu wykonawczym Komisji (UE) 2018/151[5]. Środki wskazane w tym rozporządzeniu oraz w wyliczeniu w art. 17 ust. 2 uksc mają charakter otwarty i przede wszystkim nie wskazują konkretnych rozwiązań technologicznych. Rozwiązanie takie jest podobne do rozwiązania przyjętego w regulacjach ochrony danych osobowych[6]. Zgodnie z RODO[7], administratorzy oraz podmioty przetwarzające powinny wdrożyć odpowiednie środki techniczne i organizacyjne – uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Jest to praktyczne wprowadzenie koncepcji *risk-based approach*, tj. podejścia opartego na ryzyku. Jak wskazuje się w literaturze, metoda ta polega na stosowaniu środków adekwatnych do zlokalizowanych zagrożeń, nie zaś standardowych rozwiązań wdrażanych bez analizy konkretnych procesów przetwarzania. Zastosowanie tej zasady ma też ten skutek, że RODO nie wprowadza żadnych standardowych rozwiązań, w tym ustandaryzowanej dokumentacji dotyczącej przetwarzania danych osobowych (z nielicznymi wyjątkami) (Litwiński, 2018, komentarz do art. 24 RODO). Co więcej, doktryna wskazuje, że nie jest celem regulacji ochrony

[5] Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30.01.2018 ustanawiające 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 ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ z dnia 30 stycznia 2018 r. (Dz.Urz. UE L Nr 26, s. 48); dalej: rozporządzenie wykonawcze 2018/151.

[6] Art. 24 oraz art. 32 RODO.

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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); dalej: RODO.

danych osobowych wyeliminowanie ryzyka w pełni, czego uczynić się nie da, a jedynie wdrożenie rozwiązań technicznych i organizacyjnych odpowiednich i proporcjonalnych, przy uwzględnieniu ocenianych kryteriów (Bielak-Jomma i Lubasz, 2018, komentarz do art. 32). Innymi słowy, kryterium skuteczności stosowanych środków bezpieczeństwa nie jest wskazane w art. 24 i art. 32 ust. 1 RODO. Koncepcja *risk-based approach* została również wyrażona w art. 3 uksc wskazującym, że celem krajowego systemu cyberbezpieczeństwa jest zapewnienie bezpieczeństwa, w tym przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług.

Przepisy dotyczące usług cyfrowych w uksc nakazują zarządzanie ryzykiem (art. 17 ust. 2 uksc), co z definicji (art. 2 pkt 19 uksc) oznacza, że ryzyko powinno zostać uprzednio oszacowane[8]. Wskazuje się, że przymiotnik „odpowiedni" oznacza, że nie jest możliwa budowa w stu procentach odpornego systemu. Zawsze jest to proces, który pozwala osiągnąć w danym okresie pewien poziom bezpieczeństwa. Wysokość tego poziomu musi być określona przez oszacowanie ryzyka w danej organizacji (Dysarz, 2019, Komentarz do art. 3).

Wydaje się zatem, że rozważania doktryny w zakresie ustalenia ryzyka opracowane na gruncie RODO można odpowiednio przenieść na regulacje dotyczące cyberbezpieczeństwa.

Drugą kategorią obowiązków są regulacje związane z obsługą incydentu. Dostawcy usług cyfrowych są obowiązani do podjęcia działań umożliwiających wykrycie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów (art. 18 ust. 1 pkt 1 uksc), a następnie obsługę incydentu (art. 18 ust. 1 pkt 2–7 uksc). Należy zwrócić uwagę, że wśród obowiązków dostawcy usług cyfrowych jest usuwanie podatności zidentyfikowanych w trakcie koordynacji obsługi incydentu poważnego, istotnego lub krytycznego przez właściwy CSIRT[9], a właściwy CSIRT wystąpił do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, incydentu istotnego lub krytycznego (art. 18 ust. 1 pkt 6 uksc w zw. z art. 32 ust. 2 uksc).

IV. Kontrola dostawcy usług cyfrowych

Dostawcy usług cyfrowych są nadzorowani przez organy właściwe do spraw cyberbezpieczeństwa w zakresie spełniania wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych określonych w rozporządzeniu wykonawczym 2018/151 oraz wykonywania wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych. W tym zakresie organ właściwy do spraw cyberbezpieczeństwa może przeprowadzać kontrole (art. 53 ust. 2 pkt 2 uksc).

Przepis szczególny (art. 53 ust. 3 uksc) wskazuje, że kontrola wobec dostawcy usług cyfrowych może zostać przeprowadzona dopiero po uzyskaniu dowodu, że dostawca usług cyfrowych nie spełnia wymogów określonych w rozporządzeniu wykonawczym 2018/151 lub nie wykonuje wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych (Banasiński, 2018, s. 159). Przyjęte w uksc rozwiązanie, ograniczające możliwość wszczęcia kontroli, odpowiada motywowi (60) oraz postanowieniom art. 17 ust. 1 dyrektywy NIS i jest zgodne z intencją

[8] Por. art. 20 uksc w zw. z art. 13 ust. 1 uksc, zgodnie z którymi dostawca usług cyfrowych może przekazywać do właściwego CSIRT informacje obejmujące m.in. szacowanie ryzyka.

[9] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym.

ustawodawcy europejskiego. Przedmiotowe rozwiązanie ma negatywny impakt na postawę podmiotów zobowiązanych do wdrażania obowiązków wynikających z uksc.

Do kontroli przestrzegania przepisów uksc przez dostawców usług cyfrowych będącymi przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy – Prawo przedsiębiorców[10], do niebędącymi przedsiębiorcami stosuje się zaś przepisy ustawy o kontroli w administracji rządowej[11] określające zasady i tryb przeprowadzania kontroli.

Kontrola kończy się sporządzeniem protokołu kontroli, który zawiera (art. 58 ust. 2 uksc):

1) wskazanie nazwy albo imienia i nazwiska oraz adresu podmiotu kontrolowanego;
2) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;
3) imię i nazwisko, stanowisko oraz numer upoważnienia osoby prowadzącej czynności kontrolne;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu i zakresu kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla przeprowadzonej kontroli, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości;
7) wyszczególnienie załączników.

Przed podpisaniem protokołu kontroli, dostawca usług cyfrowych w terminie 7 dni od dnia przedstawienia mu go do podpisu, może zgłosić pisemne zastrzeżenia do protokołu.

Jeżeli na podstawie ustaleń dokonanych w trakcie kontroli oraz zgromadzonych w postępowaniu kontrolnym organ właściwy do spraw cyberbezpieczeństwa uzna, że mogło dojść do naruszenia przepisów uksc przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości. Zalecenia nie są nakładane w toku postępowania administracyjnego, chociaż brakuje przepisu szczególnego wyłączającego stosowanie KPA[12]. Art. 59 ust. 2 uksc wskazuje, że od zaleceń pokontrolnych nie przysługują środki odwoławcze. Jak słusznie wskazuje się w doktrynie (Wąsowicz, 2019), wyłączenie środków odwoławczych nie jest równoznaczne z wyłączeniem prawa do wniesienia skargi do sądu administracyjnego. Dostawca usług cyfrowych, działając na podstawie art. art. 3 § 2 pkt 4 ustawy – Prawo o postępowaniu przed sądami administracyjnymi[13] może złożyć skargę do właściwego sądu administracyjnego. Podmiot kontrolowany ma obowiązek poinformowania organu właściwego do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń.

V. Kary pieniężne nakładane na dostawców usług cyfrowych

W ramach nadzoru, o którym mowa w art. 53 ust. 1 pkt 2 lit. b) uksc, organ właściwy do spraw cyberbezpieczeństwa nakłada na operatorów usług cyfrowych kary pieniężne.

Polski ustawodawca zdecydował się na ograniczenie katalogu kar nakładanych na dostawców usług cyfrowych. Katalog przewinień, za który może zostać nałożona kara administracyjna jest wąski. Zgodnie z art. 73 uksc kary pieniężne mogą być nakładane na dostawców usług cyfrowych za:

[10] Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (t.j. DzU 2019, poz. 1292, 1495), Rozdział 5. Ograniczenia Kontroli Działalności Gospodarczej.

[11] Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (DzU Nr 185, poz. 1092 ze zm.).

[12] Por. art. 7 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. z dnia 30 sierpnia 2019 r.) (DzU 2019, poz. 1781).

[13] Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. z dnia 22 listopada 2019 r.) (DzU 2019, poz. 2325).

1) niewykonanie obowiązku, o którym mowa w art. 18 ust. 1 pkt 4 uksc, czyli obowiązku zgłoszenia istotnego incydentu niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia do właściwego CSIRT;
2) niewykonane obowiązku, o którym mowa w art. 18 ust. 1 pkt 5 uksc, czyli obowiązku zapewnienia obsługi incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT, przekazując niezbędne dane, w tym dane osobowe lub
3) nieusunięcia podatności, która została zidentyfikowana w trakcie koordynacji obsługi incydentu poważnego, incydentu istotnego lub krytycznego przez właściwy CSIRT, a właściwy CSIRT wystąpił do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, incydentu istotnego lub krytycznego, zgodnie z art. 32 ust. 2 uksc.

Kary pieniężne nakładane na dostawców usług cyfrowych związane są zatem wyłącznie z sytuacjami, w których już doszło do incydentu i *de facto* niewypełnienia obowiązków informacyjnych (sprawozdawczych) lub nieusunięcia podatności zidentyfikowanej podczas obsługi incydentu. Można zauważyć, że art. 21 dyrektywy NIS uprawnia polskiego ustawodawcę do wprowadzenia sankcji również za naruszenia przepisów nakładających obowiązki związane z zapewnieniem odpowiedniego poziomu cyberbezpieczeństwa.

W przypadku stwierdzenia naruszenia prawa, organ właściwy do spraw cyberbezpieczeństwa jest obowiązany do nałożenia kary (kara nie jest fakultatywna) (Radoniewicz, 2019, komentarz do art. 74), na co wyraźnie wskazuje brzmienie art. 73 uksc (z wyjątkiem sytuacji, gdy podmiot zaprzestał wprawdzie naruszania prawa lub naprawił wyrządzoną szkodę, jednakże organ właściwy do spraw cyberbezpieczeństwa uzna, że czas trwania, zakres lub skutki naruszenia przemawiają za nałożeniem kary (Banasiński, 2018, s. 171). Odwrotnym przykładem rozróżnienia kar obligatoryjnych oraz fakultatywnych jest art. 209 ust. 1 oraz ust. 1a ustawy – Prawo telekomunikacyjne[14].

Zwraca uwagę niekonsekwencja art. 53–59 oraz art. 73 uksc. Pomimo możliwości przeprowadzenia kontroli dostawcy usług cyfrowych oraz wydania zaleceń pokontrolnych, które dostawca usług cyfrowych jest obowiązany wykonać, brak ich wykonania nie jest wprost sankcjonowany.

Regulacje krajowego systemu cyberbezpieczeństwa wyraźnie przedstawiają optykę regulacji dostawców usług cyfrowych oraz zapobiegania występowaniu incydentów z widokiem na przyszłość. Wymagania zapewnienia cyberbezpieczeństwa bez związku z konkretnym incydentem wobec dostawców usług cyfrowych są obniżone, co było świadomym wyborem ustawodawcy europejskiego.

VI. Ochrona osób fizycznych (RODO)

Naruszenie zasad cyberbezpieczeństwa przez dostawców usług cyfrowych, w szczególności obowiązków w zakresie zapewnienia odpowiedniego poziomu cyberbezpieczeństwa często, lecz nie zawsze, może wiązać się z naruszeniem zasad ochrony danych osobowych. Uzależnione to jest okoliczności czy dostawca usług cyfrowych w ramach świadczonych usług cyfrowych przetwarza dane osobowe. Należy pamiętać, że pojęcie „danych osobowych" jest bardzo szerokie

[14] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. z dnia 9 grudnia 2019 r.) (DzU 2019, poz. 2460 ze zm.).

i obejmuje różnego rodzaju informacje, które dotyczą konkretnej osoby. Mogą to być informacje, które identyfikują osobę, informacje, które odnoszą się do jej cech lub statusu osobistego lub informacje o charakterze rzeczowym (Fajgielski, 2018, s. 17; podobnie: Lubasz, 2018, s. 170).

Jak zostało wyżej wskazane, administrator danych osobowych oraz podmiot przetwarzający jest obowiązany do wdrożenia odpowiednich technicznych i organizacyjnych środków bezpieczeństwa, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.Obowiązki wynikające z RODO obejmują m.in. zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (art. 32 ust. 1 RODO). Zwraca uwagę, że obowiązek ten w znacznym stopniu odpowiada definicji cyberbezpieczeństwa (art. 2 pkt 4 uksc), zgodnie z którą cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[15]. Stąd wynika wniosek o podobieństwie obowiązków wynikających z RODO oraz uksc (Taczkowska-Olszewska, Chałubińska-Jentkiewicz i Nowikowska, 2019, cz. III rozdz. II).

Na gruncie przepisów ochrony danych osobowych Prezes UODO jest podmiotem uprawnionym do przeprowadzenia kontroli stosowania przez administratora oraz podmiot przetwarzający odpowiednich technicznych i organizacyjnych środków bezpieczeństwa.

Naruszenie obowiązków związanych z zapewnieniem odpowiednich środków bezpieczeństwa jest na gruncie RODO samodzielną okolicznością nałożenia ewentualnej kary pieniężnej, niezależnie od tego czy niezapewnienie odpowiednich środków bezpieczeństwa w konsekwencji doprowadziło do utraty poufności, integralności lub dostępności danych osobowych (art. 83 ust. 4 lit. a) RODO), czy też nie: odpowiedzialność administratora oraz podmiotu przetwarzającego za niewdrożenie odpowiednich środków bezpieczeństwa jest uniezależniona od ewentualnego wystąpienia skutku w postaci np. utraty poufności danych. Utrata poufności danych wiązać się będzie z zwiększeniem górnej granicy kary (por. art. 83 ust. 2 lit d) oraz art. 83 ust. 5 lit. a) RODO).

Należy również zwrócić uwagę na art. 82 RODO. Zgodnie z art. 82 ust. 1 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. W konsekwencji, jeżeli dojdzie do incydentu (w rozumieniu uksc) związanego z naruszeniem poufności, dostępności lub integralności przetwarzanych danych osobowych, podmiot danych może zwrócić się do dostawcy usług cyfrowych o odszkodowanie.

Z powyższego wyraźnie wynika przenikanie się regulacji dotyczących cyberbezpieczeństwa oraz ochrony danych osobowych. Jednoznacznie należy stwierdzić, że na gruncie regulacji ochrony danych osobowych dostawcy usług cyfrowych odpowiadają niezależnie od regulacji uksc.

Rozważenia wymaga czy obowiązki nałożone na dostawców usług cyfrowych w uksc oraz w rozporządzeniu wykonawczym 2018/151 powinny być brane pod uwagę podczas ustalania właściwego środka naprawczego (art. 58 ust. 2 RODO), w tym nakładania kary pieniężnej. Przepisy wprost nie odpowiadają na to pytanie. Wydaje się, że mając na uwadze wyżej opisane podobieństwo w zakresie obowiązku stosowania środków bezpieczeństwa pomiędzy RODO a uksc,

[15] Podobnie definicja „bezpieczeństwo sieci i systemów informatycznych" w art. 4 pkt 2 dyrektywy NIS.

okoliczność ta może mieć wpływ na analizę przesłanki oceny stopnia odpowiedzialności administratora lub podmiotu przetwarzającego za ewentualną wadliwość przygotowania odpowiednich środków technicznych i organizacyjnych i wdrożonych przez nich na mocy art. 25 i 32 RODO (art. 82 ust. 1 lit. d) RODO). Z kolei analiza przesłanki obowiązku oceny wszelkich innych obciążających lub łagodzących czynników mających zastosowanie do okoliczności sprawy (art. 82 ust. 1 lit. k) RODO) wskazuje, że organ nadzorczy powinien wziąć pod uwagę również inne niż wynikające z przepisów ochrony danych osobowych obowiązki związane z zapewnieniem bezpieczeństwa przetwarzania, a za takie można uznać obowiązki związane z zapewnieniem cyberbezpieczeństwa. W szczególności wszelkie dodatkowe obowiązki mogą być istotnym czynnikiem ustalenia czy organ nadzorczy zastosuje środek nadzorczy „upomnienie", czy nałoży karę pieniężną. Pamiętać jednak należy, że Prezes UODO nie ma uprawnień do kontroli przestrzegania przez dostawców usług cyfrowych przestrzegania uksc.

VII. Usługi cyfrowe jako usługi świadczone drogą elektroniczną na rzecz konsumentów

Zgodnie z definicją w uksc, usługą cyfrową jest usługa świadczona drogą elektroniczną oraz wymieniona w załączniku 2 do uksc (Lewoszewski, 2019, s. 75). Usługa świadczona drogą elektroniczną jest to usługa świadczona bez jednoczesnej obecności stron 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 ustawy – Prawo telekomunikacyjne (art. 2 pkt 4 ustawy o świadczeniu usług drogą elektroniczną[16]). Niezależnie zatem od odpowiedzialności wynikającej z uksc oraz RODO, dostawca usługi cyfrowej ponosi odpowiedzialność określoną w ustawie o świadczeniu usług drogą elektroniczną.

W ustawie o świadczeniu usług drogą elektroniczną konsekwentnie uregulowano, że „swoboda świadczenia usług drogą elektroniczną może zostać ograniczona, jeżeli jest to niezbędne ze względu na ochronę zdrowia, obronność, bezpieczeństwo państwa lub bezpieczeństwo publiczne" (art. 3b ustawy o świadczeniu usług drogą elektroniczną). Ograniczenie to znalazło odzwierciedlenie m.in. właśnie w przepisach uksc względem usług cyfrowych. Wskazuje się, że celem przedmiotowej regulacji jest wdrożenie mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń dla bezpieczeństwa cyberprzestrzeni oraz właściwemu postępowaniu w przypadku stwierdzonych incydentów oraz powszechną edukację społeczną i specjalistyczną w zakresie ochrony cyberprzestrzeni RP, również względem podmiotów niepublicznych (Chałubińska-Jentkiewicz i Taczkowska-Olszewska, 2019, komentarz do art. 3b). Innymi słowy, usługodawcy usług świadczonych drogą elektroniczną są obowiązani stosować przepisy szczególne w zakresie bezpieczeństwa określone w uksc.

Usługi cyfrowe, jeżeli są świadczone na rzecz konsumentów, podlegają obowiązkom informacyjnym określonym w art. 12 ustawy o prawach konsumenta[17]. Przepisy te nie zobowiązują dostawców usług do informowania o bezpieczeństwie świadczonych usług lub wręcz zapewniania, że świadczone usługi są bezpieczne. Brak obowiązku zapewnienia o bezpieczeństwie

[16] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. DzU 2019, poz. 123).

[17] Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (t.j. DzU 2019, poz. 134).

świadczonych usług jest spójny z obowiązkiem zapewnienia *odpowiedniego* poziomu bezpieczeństwa świadczonych usług, a bezpieczeństwa zupełnego (co jak wyżej zostało zauważone, jest faktycznie niewykonalne).

Analizując pozycję dostawcy usług cyfrowych względem konsumenta należy rozważyć czy dostawca usług cyfrowych może ograniczyć odpowiedzialność względem konsumenta za stosowanie nieodpowiednich środków bezpieczeństwa oraz czy postanowienia umowne ograniczające odpowiedzialność nie są klauzulą abuzywną. W wyroku z dnia 1 lipca 2010 r. sygn. XVII AmC 1006/09 Sąd Okręgowy w Warszawie Sąd Ochrony Konkurencji i Konsumentów uznał za niedozwolone postanowienia wzorca umowy wyłączające odpowiedzialność dostawcy usługi za „techniczne błędy programu, ingerencje osób trzecich, utraty danych przy użyciu karty z PIN-em przez osoby trzecie". Jednym z argumentów podniesionych przez Sąd było wskazanie, że, opierając się na przepisach ochrony danych osobowych, na organizatorze ciąży szczególny obowiązek stosowania środków technicznych i organizacyjnych zapewniających ochronę odpowiednią do zagrożeń. W konsekwencji Sąd uznał, że klauzula jest sprzeczna z dobrymi obyczajami (art. 385 § 1 ustawy – Kodeks cywilny[18]) i narusza uzasadnione interesy konsumentów, odpowiednia klauzula została zaś wpisana do Rejestru klauzul niedozwolonych prowadzonego przez Prezesa UOKiK[19]. Do Rejestru klauzul niedozwolonych został szereg innych postanowień, wyłączających odpowiedzialność za np.: utratę danych lub korzystanie z konta przez osoby trzecie. Wydaje się, że ewentualna próba wyłączenia odpowiedzialności dostawców usług cyfrowych również będzie stanowić niedozwolone klauzule abuzywne, w szczególności, że, podobnie jak w przywołanym orzeczeniu Sądu Okręgowego, na dostawcach usług cyfrowych ciąży szczególny obowiązek zapewnienia bezpieczeństwa świadczenia usług.

Należy również rozważyć przepisy ustawy – Kodeks cywilny oraz przepisy dotyczące odpowiedzialności producenta za produkt niebezpieczny. Stosownie do art. 449[1] ustawy – Kodeks cywilny, kto wytwarza w zakresie swojej działalności gospodarczej (producent) produkt niebezpieczny, odpowiada za szkodę wyrządzoną komukolwiek przez ten produkt. Za produkt zaś należy rozumieć (co do zasady) rzecz ruchomą. Przeważające stanowisko doktryny wskazuje, że programy komputerowe nie są objęte przedmiotową regulacją, pomimo że istnieją silne argumenty za objęciem ich reżimem odpowiedzialności za produkt niebezpieczny (Ruchała i Sikorski, 2019, komentarz do art. 4491; podobnie: Banaszczyk, 2018, komentarz do art. 4491). Przedmiotowe rozważania dotyczące programów komputerowych można przenieść na usługi cyfrowe, tj. przepisy dotyczące odpowiedzialności producenta za produkt niebezpieczny nie mogą być stosowane do usług cyfrowych, pomimo zasadności objęcia ich przedmiotową regulacją, a w szczególności w sytuacji, gdy względem usług cyfrowych nałożone są konkretne obowiązki zapewnienia bezpieczeństwa w uksc.

VIII. Podsumowanie

Regulacje zapewnienia cyberbezpieczeństwa oraz ochrony danych osobowych przenikają się i wzajemnie na siebie wpływają. Dostawca usług cyfrowych, wdrażając właściwe i proporcjonalne środki techniczne i organizacyjne, na potrzeby zapewnienia cyberbezpieczeństwa, często będzie

[18] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. DzU 2019, poz. 1145).

[19] Rejestr klauzul niedozwolonych, pozycja 2329.

podejmował działania wypełniające obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych uwzględniający ryzyko przetwarzania danych osobowych.

Odpowiedzialność usług cyfrowych za stosowanie odpowiednich (właściwych, proporcjonalnych) środków bezpieczeństwa, nawet jeżeli nie jest sankcjonowana na gruncie uksc, bardzo często będzie objęta równoległym odrębnym, reżimem regulacji na gruncie przepisów ochrony danych osobowych.

Bibliografia

Banasiński, C. (red.). (2018). *Cyberbezpieczeństwo, Zarys wykładu*. Warszawa: Wolters Kluwer.

Banasiński, C. i Nowak, W. (2018). W: C. Banasiński (red.), *Cyberbezpieczeństwo, Zarys wykładu*. Warszawa: Wolters Kluwer.

Banaszczyk, Z. (2018). W: K. Pietrzykowski (red.), *Kodeks cywilny. T. I. Komentarz. Art. 1–449[10]*. Warszawa: Wydawnictwo C.H. Beck.

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

Bielak-Jomma, E. i Lubasz, D. (2018). *RODO Ogólne Rozporządzenie o ochronie danych. Komentarz.* Warszawa: Wolters Kluwer.

Chałubińska-Jentkiewicz, K. i Taczkowska-Olszewska, J. (2019). *Świadczenie usług drogą elektroniczną. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Dysarz, J. (2019). W: A. Besiekierska (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Fajgielski, P. (2018). Komentarz do ogólnego rozporządzenia o ochronie danych. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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) (Dz.Urz. UE L 119 z 4.05.2016, s. 1, sprost.: Dz.Urz. UE L 127 z 23.05.2018, s. 2). W: P. Fajgierski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych*. Komentarz. Warszawa: Wolters Kluwer Polska.

Gutowski, M. (red.). (2019). *Kodeks cywilny. Tom II. Komentarz do art. 353–626*. Warszawa: Wydawnictwo C.H. Beck.

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

Kruk, M. (2019). Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom. *Prawo Mediów Elektronicznych*, (1).

Lewoszewski, M. (2019). Wybrane obowiązki dostawców usług cyfrowych na gruncie ustawy o cyberbezpieczeństwie. *Informacja w Administracji Publicznej*, (1).

Litwiński, P. (2018). *Ustawa o ochronie danych osobowych. Komentarz*. Warszawa: Wydawnictwo C.H. Beck.

Lubasz, D. (2018). W: E. Bielak-Jomaa, D. Lubasz (red.), *RODO Ogólne Rozporządzenie o ochronie danych. Komentarz.* Warszawa: Wolters Kluwer.

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

Rojszczak, M. (2018). W: C. Banasiński (red.), *Cyberbezpieczeństwo, Zarys wykładu*. Warszawa: Wolters Kluwer.

Ruchała, P. i Sikorski, R. (2019). W: M. Gutowski (red.), *Kodeks cywilny. Tom II. Komentarz do art. 353–626*. Warszawa: Wydawnictwo C.H. Beck.

Taczkowska-Olszewska J., Chałubińska-Jentkiewicz, K. i Nowikowska M. (2019). *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*. Warszawa: Wydawnictwo C.H. Beck.

Wąsowicz, W. (2019). W: A. Besiekierska (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz.* Warszawa: Wydawnictwo C.H. Beck, Legalis.