Paweł Pelc*

Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych

Streszczenie

Istotnym elementem bezpieczeństwa funkcjonowania w cyberprzestrzeni instytucji finansowych są odpowiednie regulacje prawne, zwłaszcza zawarte w ustawie o krajowym systemie cyberbezpieczeństwa wraz z aktami wykonawczymi oraz ustawie o usługach płatniczych stanowiących implementację unijnych regulacji, a w szczególności dyrektyw NIS i PSD2. Regulacje te są zróżnicowane dla poszczególnych typów instytucji finansowych. Uzupełnia je tzw. miękkie prawo. Ze względu na planowane zmiany w regulacjach unijnych w tym zakresie, a w szczególności planowane nowe rozporządzenie DORA i dyrektywę NIS 2.0 dojdzie do zmian regulacji prawnych dotyczących cyberbezpieczeństwa instytucji finansowych także w regulacjach krajowych.

Słowa kluczowe: instytucje finansowe, cyberbezpieczeństwo, cyberprzestrzeń, miękkie prawo, regulacje prawne

* Paweł Pelc, Akademia Sztuki Wojennej w Warszawie, Akademickie Centrum Polityki Cyberbezpieczeństwa, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

Wstęp

Doświadczenia pandemii COVID-19 pokazały jak bardzo działalność instytucji finansowych jest powiązana z cyberprzestrzenią, a jednocześnie jak istniejąca infrastruktura sieciowa pozwala tym instytucjom funkcjonować, świadczyć usługi dla swoich klientów oraz pozyskiwać nowych klientów nawet w sytuacji ograniczeń lub braku dostępu do oddziałów i centrali tych instytucji w związku z restrykcjami epidemicznymi, w tym tzw. lockdownem[1]. Część instytucji finansowych rozważa pozostawienie możliwości pracy zdalnej także po zakończeniu kryzysu związanego z pandemią[2]. Równocześnie dokonuje się wiele zmian w otoczeniu technologicznym, w którym działają instytucje finansowe, w tym w zakresie wykorzystania kryptoaktywów i tokenizowania[3] czy technologii chmurowej[4]. Zmiany te stają się powodem reakcji regulatorów[5] i nadzorców zarówno na poziomie ponadnarodowym[6], jak i krajowym[7], co zmienia otoczenie regulacyjne, w którym działają instytucje finansowe odpowiednio dostosowujące się do nowej rzeczywistości technologicznej[8] i regulacyjnej.

1 Por. P. Pelc, *The COVID-19 pandemic and the functioning of financial institutions in Poland. Cybersecurity issues*, „Cybersecurity and Law" 2020, nr 1, s. 92–101 oraz przywołane tam źródła.

2 J. Bernard, D. Golden, M. Nicholson, *Reshaping the cybersecurity landscape. How digitalization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions. Deloitte Insights*, s. 16, https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_DI_2020_FS_ISAC_Cybersecurity.pdf [dostęp: 3.09.2021].

3 Por. Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937 (COM(2020) 593 final 2020/0265(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0593&from=EN [dostęp: 18.08.2021].

4 K. Dygasiewicz, P. Zapadka, *Zasady korzystania przez banki krajowe z usługi tzw. chmury obliczeniowej społecznościowej w czasach gospodarki COVID lub postCOVID w świetle komunikatu Komisji Nadzoru Finansowego*, „Cybersecurity and Law" 2020, nr 1, s. 103–112; P. Pelc, *„Komunikat chmurowy" Komisji Nadzoru Finansowego*, ibidem, nr 2, s. 183–197.

5 Idem, *Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce*, ibidem 2021, nr 1.

6 Por. Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 (COM(2020) 595 final, 2020/0266(COD), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0596&from=EN [dostęp: 18.08.2021].

7 K. Szaniawski, *Bankowość elektroniczna w nowym otoczeniu prawnym* [w:] *Regulacje finansowe. FinTech – nowe instrumenty finansowe – resolution*, red. W. Rogowski, Warszawa 2017, s. 71–74.

8 K. Gawkowski, *Bezpieczeństwo cyberprzestrzeni w regulacjach UE*, „Teka of Political Science and International Relations" 2018, nr 2, s. 65–76.

Jednocześnie muszą się one liczyć z wieloma zagrożeniami ich działań w cyberprzestrzeni, w tym ataków takich, jak: 1) włamania do systemów banków w celu malwersacji środków czy też wykradzenia danych klientów; 2) podszywanie się pod strony firmowe w celu wyłudzenia haseł, loginów czy kodów SMS; 3) ataki typu ransomware; 4) phishing; 5) spear phishing; 6) wysyłanie maili z plikami typu malware; 7) wirusy na aplikacjach mobilnych, podobnie jak w przeglądarkach internetowych komputerów, działających również w celu wymuszenia informacji o hasłach, loginach czy kodach SMS; 8) ataki hybrydowe, które łączą w sobie kilka technik[9].

Ataki te nie ustają[10] mimo działań podejmowanych przez instytucje finansowe w celu zabezpieczenia się przed nimi i edukowania ich klientów[11], a także oczekiwań formułowanych w tym zakresie przez Komisję Nadzoru Finansowego[12]. O skali zagrożeń związanych z cyberbezpieczeństwem instytucji finansowych z punktu widzenia organu nadzoru może świadczyć wyodrębnienie w strukturach Urzędu Komisji Nadzoru Finansowego jeszcze przed pandemią COVID-19 Departamentu Cyberbezpieczeństwa[13]. Kwestie te są szczególnie istotne ze względu na to, że działalność instytucji finansowych opiera się na zaufaniu ich klientów, dlatego niezbędne jest takie uregulowanie ich działalności, żeby je zapewniało, stąd zarówno uregulowania dotyczące tajemnicy zawodowej w instytucjach finansowych[14], jak i mechanizmów zarządzania ryzykiem w ich działalności, w tym w sferze cyberprzestrzeni.

9 R. Pitera, *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, „Przegląd Nauk o Obronności" 2017, nr 4, s. 181–192.

10 Por. R. Lakshmanan, *Cybercrimilals Behind Mekotio and Grandoreiro Bankin Trojan Arrested in Spain*, https://thehackernews.com/2021/07/16-cybercriminals-behind-mekotio-and.html?mod=djemCybersecruityPro&tpl=cy [dostęp: 18.08.2021].

11 *Bezpieczne bankowanie*, https://zbp.pl/dla-klientow/bezpieczne-bankowanie/Aktualnosci [dostęp: 18.08.2021]; *Cyberbezpieczeństwo w praktyce*, https://zbp.pl/dla-klientow/Bankowcy-dla-edukacji/Cyberbezpieczenstwo-w-praktyce [dostęp: 18.08.2021].

12 *Cyberbezpieczeństwo elektronicznych kanałów dostępu do usług bankowych – list przewodniczącego KNF do sektora bankowego*, https://www.knf.gov.pl/knf/pl/komponenty/img/Cyberbezpieczenstwo_elektronicznych_kanalow_dostepu_do_uslug_bankowych%E2%80%93list_Przewodniczacego_KNF_do_sektora_bankowego_72587.pdf [dostęp: 18.08.2021].

13 K. Mroczka, *Cyberbezpieczeństwo w systemie finansowym – perspektywa nadzorcza*, s. 8–9, https://www.knf.gov.pl/knf/pl/komponenty/img/Cyberbezpieczenstwo_w_systemie_finansowym_perspektywa_nadzorcza_73892.pdf [dostęp: 18.08.2021].

14 P. Pelc, *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, nr 2, s. 151–164.

Instytucje finansowe w krajowym systemie cyberbezpieczeństwa

Z tych przyczyn instytucje finansowe są elementem krajowej systemu cyberbezpieczeństwa. Zgodnie z art. 4 pkt 1, 9 i 10 ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa[15] system ten obejmuje m.in. operatorów usług kluczowych, Narodowy Bank Polski i Bank Gospodarstwa Krajowego.

Narodowy Bank Polski i Bank Gospodarstwa Krajowego, zgodnie z art. 21 ust. 1, art. 22 ust. 1, art. 23 ust. 2–5, art. 24–25 rzeczonej ustawy są podmiotami publicznymi, na których ciążą określone w tych przepisach obowiązki związane z wyznaczeniem osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zarządzania, zgłaszania i obsługi incydentów[16].

Operatorem usługi kluczowej zgodnie z art. 5 ust. 1 ustawy jest podmiot, o którym mowa w załączniku nr 1 do tejże ustawy, mający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. W załączniku nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa wyodrębniono sektor „bankowość i infrastruktura rynków finansowych", w którego ramach uznano za podmioty mogące być uznane za operatorów usług kluczowych instytucje kredytowe w rozumieniu przepisów prawa bankowego[17], banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, spółdzielcze kasy oszczędnościowo-kredytowe, podmioty prowadzące rynki regulowane w rozumieniu przepisów o obrocie instrumentami finansowymi[18], CCP (osobę prawną, która działa pomiędzy kontrahentami kontraktów będących w obrocie na co najmniej jednym rynku finansowym, stając się nabywcą dla każdego sprzedawcy i sprzedawcą dla każdego nabywcy) oraz spółkę akcyjną będącą podmiotem zależnym od Krajowego Depozytu Papierów Wartościowych SA, której on przekazał na podstawie pisemnej umowy wykonywanie czynności z zakresu swoich ustawowych

15 Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j., Dz.U. 2020, poz. 1369.

16 Więcej na temat obowiązków podmiotów publicznych w ustawie o krajowym systemie cyberbezpieczeństwa zob. M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, nr 2, s. 57–72.

17 Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, t.j., Dz.U. 2020, poz. 1896.

18 Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, t.j. ibidem 2021, poz. 328.

zadań. Oznacza to, że jedynie część sektora finansowego została uznana przez ustawodawcę za element krajowego systemu cyberbezpieczeństwa i w efekcie część instytucji finansowych nie jest zaliczana do kategorii, które mogą być uznane za operatorów usług kluczowych. Na te instytucje finansowe, które zostały uznane za operatorów usługi kluczowej, nałożono obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej (art. 8 ustawy o krajowym systemie cyberbezpieczeństwa), wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, a także zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy w zakresie zagrożeń cyberbezpieczeństwa (art. 9 ustawy o krajowym systemie cyberbezpieczeństwa), opracowania, wdrożenia i aktualizacji dokumentacji cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 10 ustawy o krajowym systemie cyberbezpieczeństwa), obsługi incydentów, zgłaszania incydentów poważnych i współdziałania przy obsłudze incydentu poważnego i incydentu krytycznego (art. 11 ustawy o krajowym systemie cyberbezpieczeństwa), powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcia umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (art. 14 ustawy o krajowym systemie cyberbezpieczeństwa), a także zapewnienia przeprowadzenia, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 15 ustawy o krajowym systemie cyberbezpieczeństwa).

W rozporządzeniu Rady Ministrów z 11 września 2018 roku w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[19] wydanym na postawie art. 11 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa w sektorze „bankowość i infrastruktura rynków finansowych" określono jako usługi kluczowe przyjmowanie depozytów pieniężnych lub innych funduszy podlegających zwrotowi od klientów; udzielanie kredytów na swój własny rachunek przez instytucję kredytową, wykonywanie przez bank lub oddział banku zagranicznego następujących czynności: 1) przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów lub 2) prowadzenie innych rachunków bankowych, lub 3) udzielanie

19 Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, ibidem 2018, poz. 1806.

kredytów, lub 4) przeprowadzanie bankowych rozliczeń pieniężnych, lub 5) udzielanie pożyczek pieniężnych, lub 6) świadczenie usług płatniczych oraz wydawanie pieniądza elektronicznego, lub 7) terminowe operacje finansowe, lub 8) nabywanie i zbywanie wierzytelności pieniężnych, lub 9) wykonywanie czynności zleconych, związanych z emisją papierów wartościowych, lub 10) dokonywanie obrotu papierami wartościowymi, lub 11) świadczenie usług zaufania oraz wydawanie środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania, lub 12) przyjmowanie wpłat gotówki i dokonywanie wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku, lub 13) wykonywanie transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy: a) przez wykonywanie usług polecenia zapłaty, w tym jednorazowych poleceń zapłaty, b) przy użyciu karty płatniczej lub podobnego instrumentu płatniczego, c) przez wykonywanie usług polecenia przelewu, w tym stałych zleceń, lub 14) wykonywanie transakcji płatniczych wymienionych w pkt 13, w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, a w przypadku instytucji płatniczej lub instytucji pieniądza elektronicznego – kredytu, o którym mowa w art. 74 ust. 3 lub art. 132j ust. 3 ustawy z 19 sierpnia 2011 roku o usługach płatniczych[20], lub 15) wydawanie instrumentów płatniczych, lub 16) umożliwianie akceptowania instrumentów płatniczych oraz wykonywania transakcji płatniczych, zainicjowanych instrumentem płatniczym płatnika przez akceptanta lub za jego pośrednictwem, polegających w szczególności na obsłudze autoryzacji, przesyłaniu do wydawcy instrumentu płatniczego lub systemów płatności zleceń płatniczych płatnika lub akceptanta, mających na celu przekazanie akceptantowi należnych mu środków, z wyłączeniem czynności polegających na rozliczaniu i rozrachunku tych transakcji w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku (*acquiring*), lub 17) świadczenie usługi inicjowania transakcji płatniczej, wykonywanie przez oddział instytucji kredytowej jednej z czynności bankowych, o których mowa w art. 5 ust. 1 pkt 1–3, 6 oraz ust. 2 pkt 1 i 2 prawa bankowego[21], wykonywanie przez spółdzielcze kasy

20 Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, t.j., ibidem 2020, poz. 794.

21 Przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów; prowadzenie innych rachunków bankowych; udzielanie kredytów; przeprowadzanie bankowych rozliczeń pieniężnych; udzielanie pożyczek pieniężnych; operacje czekowe i wekslowe oraz operacje, których przedmiotem są warranty.

oszczędnościowo-kredytowe czynności, o których mowa w art. 3 ustawy z 5 listopada 2009 roku o spółdzielczych kasach oszczędnościowo-kredytowych[22] w zakresie określonym w tym przepisie[23], prowadzenie przez podmiot prowadzący rynek regulowany rynku regulowanego lub innej działalności w zakresie organizowania obrotu instrumentami finansowymi oraz giełdy towarowej, organizowanie alternatywnego systemu obrotu instrumentami finansowymi, działanie pomiędzy kontrahentami kontraktów będących w obrocie na co najmniej jednym rynku finansowym, polegające na staniu się nabywcą dla każdego sprzedawcy i sprzedawcą dla każdego nabywcy (CCP), a w przypadku spółki akcyjnej powołanej przez KDPW SA prowadzenie rozliczeń i transakcji zawieranych w obrocie instrumentami finansowymi.

Instytucje finansowe będące operatorami usług kluczowych muszą zapewnić warunki organizacyjne i techniczne określone w rozporządzeniu Ministra Cyfryzacji z 4 grudnia 2019 roku w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo[24]. Zgodnie z postanowieniami tego rozporządzenia wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo są obowiązane spełniać następujące warunki techniczne: dysponować sprzętem komputerowym oraz wyspecjalizowanymi narzędziami informatycznymi umożliwiającymi rejestrowanie zgłoszeń incydentów, analizę kodu oprogramowania uznanego za szkodliwe, badanie odporności systemów informacyjnych na przełamanie lub ominięcie zabezpieczeń, zabezpieczanie informacji potrzebnych do analizy powłamaniowej pozwalające na określenie wpływu incydentu poważnego na

22 Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, t.j., ibidem 2020, poz. 1643.

23 Gromadzenie środków pieniężnych wyłącznie swoich członków, udzielanie im pożyczek i kredytów, przeprowadzanie na ich zlecenie rozliczeń finansowych oraz wykonywanie dystrybucji ubezpieczeń, pośredniczenie w zbywaniu i odkupywaniu jednostek uczestnictwa funduszy inwestycyjnych lub tytułów uczestnictwa funduszy zagranicznych oraz funduszy inwestycyjnych otwartych z siedzibą w państwach należących do Europejskiego Obszaru Gospodarczego, wydawanie pieniądza elektronicznego na rzecz członków kas, świadczenie na rzecz swoich członków usługi zaufania oraz wydawanie swoim członkom środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania oraz identyfikacji elektronicznej.

24 Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, ibidem 2019, poz. 2479.

świadczenie usługi kluczowej w zakresie określonym w rozporządzeniu, dysponować redundantnymi środkami łączności umożliwiającymi prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczą usługi, oraz właściwym zespołem reagowania na incydenty bezpieczeństwa komputerowego działającym na poziomie krajowym. Nałożono na nie także obowiązek zabezpieczenia pomieszczenia lub zespołu pomieszczeń adekwatnie do przeprowadzonego szacowania ryzyka odpowiednie do przetwarzanych informacji, spełniające wymogi minimalne określone w rozporządzeniu i umożliwiające wypełnienie obowiązków określonych w tym rozporządzeniu.

Rozwiązania te są elementem regulacji mających na celu zwiększenie cyberbezpieczeństwa instytucji objętych tymi regulacjami. Również część regulacji sektorowych dotyczy kwestii cyberbezpieczeństwa instytucji finansowych niezależnie od tego, czy są operatorami usług kluczowych w ramach krajowego systemu cyberbezpieczeństwa.

Bezpieczeństwo świadczenia usług płatniczych

Zgodnie z art. 3 ust. 1 ustawy o usługach płatniczych przez usługi płatnicze rozumie się działalność polegającą na: 1) przyjmowaniu wpłat gotówki i dokonywaniu wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku; 2) wykonywaniu transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy: a) przez wykonywanie usług polecenia zapłaty, w tym jednorazowych poleceń zapłaty, b) przy użyciu karty płatniczej lub podobnego instrumentu płatniczego, c) przez wykonywanie usług polecenia przelewu, w tym stałych zleceń; 3) wykonywaniu transakcji płatniczych wymienionych w pkt 2, w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, a w przypadku instytucji płatniczej lub instytucji pieniądza elektronicznego – kredytu, o którym mowa w art. 74 ust. 3 lub art. 132j ust. 3 ustawy o usługach płatniczych; 4) wydawaniu instrumentów płatniczych; 5) umożliwianiu akceptowania instrumentów płatniczych oraz wykonywania transakcji płatniczych, zainicjowanych instrumentem płatniczym płatnika przez akceptanta lub za jego pośrednictwem, polegających w szczególności na obsłudze autoryzacji, przesyłaniu do wydawcy instrumentu płatniczego lub systemów płatności zleceń płatniczych płatnika lub akceptanta, mających na celu przekazanie akceptantowi należnych mu środków, z wyłączeniem czynności polegających na rozliczaniu i rozrachunku tych transakcji

w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku (*acquiring*); 6) świadczeniu usługi przekazu pieniężnego; 7) świadczeniu usługi inicjowania transakcji płatniczej; 8) świadczeniu usługi dostępu do informacji o rachunku.

Artykuł 4 ust. ustawy o usługach płatniczych określa, że dostawcą usług płatniczych może być wyłącznie bank krajowy, oddział banku zagranicznego, instytucja kredytowa w rozumieniu prawa bankowego, oddział instytucji kredytowej, instytucja pieniądza elektronicznego i oddział instytucji pieniądza elektronicznego – w przypadku, gdy oddział znajduje się w państwie członkowskim, a siedziba takiej instytucji pieniądza elektronicznego znajduje się poza państwem członkowskim, o ile usługi płatnicze świadczone przez oddział są związane z wydawaniem pieniądza elektronicznego, oddział podmiotu świadczącego w innym niż Rzeczpospolita Polska państwie członkowskim, zgodnie z prawem tego państwa, pocztowe usługi płatnicze, uprawnionego zgodnie z prawem tego państwa do świadczenia usług płatniczych oraz Poczta Polska Spółka Akcyjna w zakresie, w jakim odrębne przepisy upoważniają ją do świadczenia usług płatniczych, instytucja płatnicza, Europejski Bank Centralny, Narodowy Bank Polski oraz bank centralny państwa członkowskiego innego niż Rzeczpospolita Polska – w przypadku, gdy nie działają w charakterze władz monetarnych lub organów administracji publicznej, organ administracji publicznej, spółdzielcza kasa oszczędnościowo-kredytowa lub Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa w zakresie, w jakim odrębne przepisy uprawniają je do świadczenia usług płatniczych, biuro usług płatniczych, mała instytucja płatnicza oraz dostawca świadczący wyłącznie usługę dostępu do informacji o rachunku.

Artykuł 32f–32h ustawy o usługach płatniczych nakłada na dostawców usług płatniczych obowiązek podejmowanych przez dostawcę usług płatniczych w ramach systemu zarządzania ryzykiem podejmowania środków ograniczających ryzyko oraz wprowadzenia mechanizmów kontroli służących zarządzaniu ryzykiem operacyjnym oraz ryzykiem naruszenia bezpieczeństwa w zakresie świadczenia usług płatniczych, niezwłocznego informowania o poważnych incydentach operacyjnych i incydentach związanych z bezpieczeństwem, w tym o charakterze teleinformatycznym, oraz rocznych danych dotyczących oszustw związanych z wykonywanymi usługami płatniczymi, uwzględniając różne sposoby świadczenia usług płatniczych. Ponadto art. 38i tejże ustawy nakłada na dostawców usług płatniczych obowiązek stosowania silnego uwierzytelniania użytkownika.

Regulacja ta, podobnie jak regulacja dotycząca krajowego systemu cyberbezpieczeństwa, ma zastosowanie jedynie do części instytucji finansowych i jest związana z oferowaniem przez nie usług płatniczych.

„Miękkie prawo"

Istotny wpływ na działalność instytucji finansowych w zakresie cyberbezpieczeństwa ma tzw. miękkie prawo[25], czyli różnego rodzaju rekomendacje i wytyczne organów nadzoru wydawane na podstawie stosownych upoważnień lub bez nich[26]. Co do zasady nie są one źródłami prawa obowiązującymi w Polsce, nie można jednak pominąć ich wpływu na funkcjonowanie instytucji nadzorczych. Komisja Nadzoru Finansowego wydała wiele wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego adresowanych do powszechnych towarzystw emerytalnych, zakładów ubezpieczeń i reasekuracji, towarzystw funduszy inwestycyjnych, podmiotów infrastruktury rynku kapitałowego oraz firm inwestycyjnych. Ponadto Komisja Nadzoru Finansowego wydała dla banków rekomendację D dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach oraz rekomendację M dotyczącą zarządzania ryzykiem operacyjnym w bankach, a dla spółdzielczych kas oszczędnościowo-kredytowych rekomendację D-SKOK dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych. Ponadto wydała ona rekomendację dotyczącą bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe. Ponadto Europejski Bank Centralny wydał rekomendacje dotyczące bezpieczeństwa płatności internetowych.

25 Z. Ofiarski, *Rola soft law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego* [w:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, red. A. Jurkowska-Zeidler, M. Olszak, Warszawa 2016, s. 137–160; C. Banasiński, *Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa* [w:] *Cyberbezpieczeństwo*, red. C. Banasiński, M. Rojszczak, Warszawa 2020, s. 30–31.

26 P. Pelc, *Nadzór Komisji Nadzoru Finansowego nad spółdzielczymi kasami oszczędnościowo-kredytowymi i Kasą Krajową oraz instrumenty nadzorcze Komisji Nadzoru Finansowego w stosunku do kas i Kasy Krajowej* [w:] *Prawo spółdzielcze. Zagadnienia materialnoprawne i procesowe*, red. A. Herbet, J. Misztal-Konecka, P. Zakrzewski, Lublin 2017, s. 255–261.

Komisja Nadzoru Finansowego w swojej działalności nadzorczej w stosunku do części instytucji finansowych (banki[27], zakłady ubezpieczeń i zakłady reasekuracji, powszechne towarzystwa emerytalne, firmy inwestycyjne i towarzystwa funduszy inwestycyjnych) stosuje tzw. metodologię BION, czyli badanie i ocenę nadzorczą. Jest to element nadzoru opartego na ocenie ryzyka. Pierwotnie był to system wdrożony dla banków przez nadzór bankowy. Ocena w ramach tego systemu obejmuje zarządzanie ryzykiem, w tym wdrażanie procedur rozpoznawania i ograniczania ryzyka.

Zakończenie

Regulacje dotyczące cyberbezpieczeństwa instytucji finansowych nie są jednolite dla wszystkich instytucji finansowych. Zależą one zarówno od charakteru, jak i od skali prowadzonej przez nie działalności, a także od rodzaju instytucji finansowej. Regulacje prawne w tym zakresie są uzupełniane przez tzw. miękkie prawo. Znaczna część polskich regulacji dotyczących cyberbezpieczeństwa instytucji finansowych to zaimplementowane regulacje unijne, w tym w szczególności tzw. dyrektywy NIS[28] oraz PSD2[29]. Zapoczątkowany przez Komisję Europejską proces zmian zarówno w dyrektywie NIS (wniosek w sprawie tzw. dyrektywy NIS 2.0[30]), jak i w dyrektywie PSD2[31] wymusi zmiany zarówno w ustawie o krajowym systemie cyberbezpieczeństwa, jak

27 *Metodyka badania i oceny nadzorczej banków komercyjnych, zrzeszających oraz spółdzielczych (Metodyka BION)*, Warszawa 2021, https://www.google.pl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjXj9i29efxAhXeAhAIHT5LAe4QFnoECBwQAA&url=https%3A%2F%2Fwww.knf.gov.pl%2Fknf%2Fpl%2Fkomponenty%2Fimg%2FMetodyka_BION_bankow_2021_73447.pdf&usg=AOvVaw3JyqMy1MDS-1SAuJNjuhbm1 [dostęp: 18.08.2021].

28 Dyrektywa 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 2016, L 194/1.

29 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, ibidem 2015, L 335/35.

30 Proposal for a Directive of the European Parliament and of the council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final 2020/0359 (COD), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166 [dostęp: 18.08.2021].

31 Wniosek. Dyrektywa Parlamentu Europejskiego i Rady zmieniająca dyrektywy 2006/43/WE, 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366

i ustawie o usługach płatniczych. Ponadto w ramach tzw. pakietu finansów cyfrowych Komisja Europejska zaproponowała przyjęcie nowego, adresowanego przede wszystkim do instytucji finansowych, rozporządzenia[32] wymuszającego zwiększenie bezpieczeństwa ich funkcjonowania i zarządzania ryzykiem także w sferze cyberbezpieczeństwa[33], zastosowanie zasady proporcjonalności. Wszystkie te działania wpłyną niewątpliwie na zakres regulacji prawnych dotyczących zarządzania cyberbezpieczeństwem instytucji finansowych i częściowo zmniejszą odmienności w tym zakresie, to jednak m.in. zastosowanie w projekcie DORA zasady proporcjonalności pozostawi w dalszym ciągu odrębności między poszczególnymi instytucjami finansowymi i pozwoli uwzględnić specyfikę ich działania.

Bibliografia

Banasiński C., *Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa* [w:] *Cyberbezpieczeństwo*, red. C. Banasiński, M. Rojszczak, Warszawa 2020.

Bernard J., Golden D., Nicholson M., *Reshaping the cybersecurity landscape. How digitalization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions. Deloitte Insights*, https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_DI_2020_FS_ISAC_Cybersecurity.pdf [dostęp: 3.09.2021].

Dygasiewicz K., Zapadka P., *Zasady korzystania przez banki krajowe z usługi tzw. chmury obliczeniowej społecznościowej w czasach gospodarki COVID lub postCOVID w świetle komunikatu Komisji Nadzoru Finansowego*, „Cybersecurity and Law" 2020, nr 1.

Gawkowski K., *Bezpieczeństwo cyberprzestrzeni w regulacjach UE*, „Teka of Political Science and International Relations" 2018, nr 2.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, nr 2.

Lakshmanan R., *Cybercrimilals Behind Mekotio and Grandoreiro Bankin Trojan Arrested in Spain*, https://thehackernews.com/2021/07/16-cybercriminals-behind-mekotio-and.html?mod=djemCybersecruityPro&tpl=cy [dostęp: 18.08.2021].

Mroczka K., *Cyberbezpieczeństwo w systemie finansowym – perspektywa nadzorcza*, https://www.knf.gov.pl/knf/pl/komponenty/img/Cyberbezpieczenstwo_w_systemie_finansowym_perspektywa_nadzorcza_73892.pdf [dostęp: 18.08.2021].

Ofiarski Z., *Rola soft law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego* [w:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, red. A. Jurkowska-Zeidler, M. Olszak, Warszawa 2016.

Pelc P., *„Komunikat chmurowy" Komisji Nadzoru Finansowego*, „Cybersecurity and Law" 2020, nr 2.

i (UE) 2016/2341, COM(2020) 596 final, 2020/0268(COD) (https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0596&from=EN [dostęp: 18.08.2021].

32 Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014, COM(2020) 595 final, 2020/0266(COD), (https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0595&from=EN [dostęp: 18.08.2021].

33 P. Pelc, *Wpływ planowanych przez UE działań...*

Pelc P., *Nadzór Komisji Nadzoru Finansowego nad spółdzielczymi kasami oszczędnościowo-kredytowymi i Kasą Krajową oraz instrumenty nadzorcze Komisji Nadzoru Finansowego w stosunku do kas i Kasy Krajowej* [w:] *Prawo spółdzielcze. Zagadnienia materialnoprawne i procesowe*, red. A. Herbet, J. Misztal-Konecka, P. Zakrzewski, Lublin 2017.
Pelc P., *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, nr 2.
Pelc P., *The COVID-19 pandemic and the functioning of financial institutions in Poland. Cybersecurity issues*, „Cybersecurity and Law" 2020, nr 1.
Pelc P., *Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce*, „Cybersecurity and Law" 2021, nr 1.
Pitera R., *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, „Przegląd Nauk o Obronności" 2017, nr 4.
Szaniawski K., *Bankowość elektroniczna w nowym otoczeniu prawnym* [w:] *Regulacje finansowe. FinTech – nowe instrumenty finansowe – resolution*, red. W. Rogowski, Warszawa 2017.

Selected regulations on cybersecurity of financial institutions

Abstract

An important element of the security of the functioning of financial institutions in cyberspace are the relevant legal regulations, in particular those contained in the Act on the national cybersecurity system together with executive acts and the Act on payment services, which are the implementation of EU regulations, in particular the NIS and PSD2 directives. These regulations differ for individual types of financial institutions. They are complemented by the so-called soft law. Due to the planned changes in EU regulations in this area, in particular the planned new DORA regulation and the NIS 2.0 directive, there will be changes in the legal regulations regarding cybersecurity of financial institutions also in national regulations

Key words: financial institutions, cybersecurity, cyberspace, soft law, legal regulations