Paweł Pelc*

Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa

Streszczenie

Regulacje dotyczące rynku finansowego zawierają regulacje dotyczące tajemnicy zawodowej, w tym tajemnicy bankowej, przy czym brak jest jednolitej regulacji – dla każdego typu instytucji finansowej regulacja w tym zakresie jest odrębna. Tajemnica zawodowa nie jest jednak bezwzględna i ustawodawca określa zasady jej udostępniania i wymiany z innymi podmiotami. Część instytucji finansowych może być operatorami usług kluczowych w ramach krajowego systemu cyberbezpieczeństwa, część może być traktowana jako dostawcy usług cyfrowych, a dwie Bank Gospodarstwa Krajowego i Narodowy Bank Polski są podmiotami publicznymi stanowiącymi część krajowego systemu cyberbepieczeństwa. Elementem cyberbezpieczeństwa jest także zachowanie poufności, zatem w przypadku przetwarzania informacji stanowiących tajemnicę zawodową w systemach informacyjnych zastosowanie mogą mieć także regulacje dotyczące krajowego systemu cyberbezpieczeństwa. Mimo nietożsamych celów stosowanie regulacji dotyczących tajemnicy zawodowej i regulacji dotyczących cyberbezpieczeństwa może się wzajemnie wzmacniać, czemu dodatkowo może sprzyjać stosowanie odrębnej regulacji przyjętej na szczeblu europejskim w zakresie ochrony danych osobowych.

Słowa kluczowe: cyberbezpieczeństwo, tajemnica zawodowa, tajemnica bankowa, instytucja finansowa, rynek finansowy

* Paweł Pelc, Akademia Sztuki Wojennej w Warszawie, Centrum Badań nad Bezpieczeństwem, Ośrodek Centrum Studiów nad Cyberbezpieczeństwem, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

Instytucje działające na rynku finansowym swoją działalność w dużym stopniu opierają na zaufaniu, jakim obdarzają je ich klienci. Utrata zaufania rodzi ryzyko niewypłacalności takich instytucji, na przykład w razie wystąpienia tzw. runu na banki, czyli klasycznej paniki bankowej[1], stąd w systemach finansowych podejmowane są różne działania mające na celu zachowanie zaufania do instytucji finansowych. Do działań tych należą różnego rodzaju systemy ochrony klientów instytucji finansowych (w tym w szczególności gwarantujące ich depozyty na wypadek upadłości banków lub innych instytucji kredytowych[2]), nadzór nad nimi oraz mechanizmy zapewnienia płynności zwłaszcza instytucjom depozytowym. Oprócz powyższych mechanizmów ochronnych, czynnikiem budowania zaufania do instytucji rynku finansowego umożliwiającym wykonywanie ich funkcji jest także kwestia ochrony informacji o klientach przyjmująca postać tajemnicy bankowej[3] lub innych form tajemnicy zawodowej. Chronione są zarówno informacje pozyskane przez instytucje rynku finansowego, jak i przez podmioty publiczne, w szczególności tworzące. tzw. sieć bezpieczeństwa finansowego, czyli Komisję Nadzoru Finansowego, Narodowy Bank Polski, Ministra Finansów i Bankowy Fundusz Gwarancyjny[4].

Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym[5] nie zawiera definicji rynku finansowego, a nadzór nad rynkiem finansowym definiuje jako m.in. nadzór bankowy, emerytalny, ubezpieczeniowy, nad rynkiem kapitałowym, instytucjami płatniczymi, małymi instytucjami płatniczymi, dostawcami świadczącymi wyłącznie usługę dostępu do informacji o rachunku, biurami usług płatniczych, instytucjami pieniądza elektronicznego, oddziałami zagranicznych instytucji pieniądza elektronicznego, agencjami ratingowymi, spółdzielczymi kasami oszczędnościowo-kredytowymi i Krajową Spółdzielczą Kasą Oszczędnościowo-Kredytową poprzez odwołanie do regulacji dotyczących poszczególnych segmentów rynku finansowego. Nie każdy podmiot

1 Por. M. Iwanicz-Drozdowska (red.), *Kryzysy bankowe. Przyczyny i rozwiązania*, Warszawa 2002; T. Obal, *System gwarantowania depozytów w USA* [w:] W. Baka (red.), *Systemy gwarantowania depozytów w Polsce i na świecie. Dziesięć lat Bankowego Funduszu Gwarancyjnego*, Warszawa 2005, s. 187–188.

2 W Polsce takimi instytucjami są także spółdzielcze kasy oszczędnościowo-kredytowe, w których depozyty ich członków zostały objęte ochroną przez Bankowy Fundusz Gwarancyjny w 2013 r. w wyniku nowelizacji ustawy o spółdzielczych kasach oszczędnościowo-kredytowych oraz wówczas obowiązującej ustawy o Bankowym Funduszu Gwarancyjnym.

3 J. Byrski, *Tajemnica prawnie chroniona w działalności bankowej*, Legalis 2010.

4 K. Stępień, *Instytucje Sieci Bezpieczeństwa Finansowego w Polsce z perspektywy instrumentów zapewniających stabilność finansową*, „Roczniki Ekonomii i Zarządzania" 2017, nr 3, s. 48.

5 T.j. Dz.U. z 2020 r., poz. 180 ze zm.

podlegający nadzorowi Komisji Nadzoru Finansowego może być uznany za instytucję finansową – w szczególności nie można bowiem uznać za instytucje finansowe emitentów papierów wartościowych.

Regulacje dotyczące tajemnicy zawodowej zawierają ustawy regulujące funkcjonowanie instytucji sieci bezpieczeństwa finansowego. W przypadku Narodowego Banku Polskiego Pracownicy NBP oraz członkowie Rady i organów opiniodawczo-doradczych przy Zarządzie NBP są obowiązani do nieujawniania osobom nieupoważnionym informacji, z którymi zapoznali się w trakcie wykonywania swoich obowiązków, w tym informacji objętych tajemnicą bankową na podstawie ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, informacji objętych ochroną na podstawie przepisów dotyczących ochrony informacji niejawnych, jak również innych informacji chronionych ustawowo. Obowiązek ten trwa również po rozwiązaniu stosunku pracy, a także po ustaniu członkostwa w Radzie lub wspomnianych wyżej organach[6]. W odniesieniu do Komisji Nadzoru Finansowego przewodniczący Komisji Nadzoru Finansowego, jego zastępcy, członkowie Komisji Nadzoru Finansowego, pracownicy Urzędu Komisji Nadzoru Finansowego i osoby zatrudnione w Urzędzie Komisji na podstawie umowy o dzieło, umowy zlecenia albo innych umów o podobnym charakterze są obowiązani, na podstawie art. 16 ust. 1 ustawy o nadzorze nad rynkiem finansowym do nieujawniania osobom nieupoważnionym informacji chronionych na podstawie odrębnych ustaw. Obowiązek ten trwa również po ustaniu pełnienia funkcji, rozwiązaniu stosunku pracy lub rozwiązaniu umowy o dzieło, umowy zlecenia albo innych umów o podobnym charakterze.

W konsekwencji należy wskazać, że szczegółowa regulacja dotycząca tajemnicy w instytucjach finansowych, określona jest przede wszystkim w regulacjach dotyczących funkcjonowania tych instytucji. Niezależnie od zachowania tajemnicy instytucje rynku finansowego muszą także stosować się do reguł dotyczących przetwarzania danych osobowych[7].

Zgodnie z art. 104 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe[8] tajemnica bankowa określona jest następująco: bank, osoby w nim zatrudnione

6 Art. 55 ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (t.j. Dz.U. z 2019 r., poz. 1810 ze zm.).

7 J. Byrski, L. Sytniewski, *Zmiany w praktyce działania instytucji finansowych na skutek ogólnego rozporządzenia o ochronie danych. Wybrane zagadnienia prawne* [w:] W. Rogowski (red.), *Regulacje Finansowe. FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017, s. 77–92; M. Krzysztofek, *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, LEX 2015.

8 T.j. Dz.U. z 2019 r., poz. 2357 ze zm.

oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje.

Norma ta ma także zastosowanie do oddziałów banków z innych krajów Unii Europejskiej oraz spoza niej[9]. Na tajemnicy bankowej w dużym stopniu wzorowane są także rozwiązania dotyczące tajemnicy w regulacjach dotyczących innych instytucji finansowych.

Najbliższą do działalności banków jest działalność spółdzielczych kas oszczędnościowo-kredytowych. Zgodnie z art. 9e ust. 1 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych[10] spółdzielcza kasa oszczędnościowo-kredytowa jest obowiązana do zachowania tajemnicy zawodowej obejmującej wszystkie informacje dotyczące czynności, o których mowa w art. 3 ust. 1 tej ustawy (czyli gromadzenie środków pieniężnych wyłącznie swoich członków, udzielanie im pożyczek i kredytów, przeprowadzanie na ich zlecenie rozliczeń finansowych oraz wykonywanie dystrybucji ubezpieczeń), w tym także informacje uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której kasa tę czynność wykonuje.

Zgodnie z art. 35 ust. 1 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej[11] zakład ubezpieczeń i osoby w nim zatrudnione, a także osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia.

W odniesieniu do działalności funduszy inwestycyjnych tajemnica zawodowa została określona w art. 280 ust. 1 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi[12] tajemnicą zawodową jest tajemnica obejmująca informację uzyskaną w związku z podejmowanymi czynnościami służbowymi w ramach zatrudnienia, stosunku zlecenia lub innego stosunku prawnego o podobnym charakterze, dotyczącą chronionych prawem interesów podmiotów dokonujących czynności związanych z działalnością funduszu inwestycyjnego, alternatywnej spółki inwestycyjnej, funduszu zagranicznego, unijnego AFI lub zbiorczego

9 M. Krzysztofek, *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, LEX 2015.
10 T.j. Dz.U. z 2019 r., poz. 2412 ze zm.
11 T.j. Dz.U. z 2019 r., poz. 381 ze zm.
12 T.j. Dz.U. z 2020 r., poz. 95 ze zm.

portfela papierów wartościowych, w szczególności z lokatami oraz rejestrem uczestników funduszu inwestycyjnego, alternatywnej spółki inwestycyjnej, funduszu zagranicznego, unijnego AFI lub zbiorczego portfela papierów wartościowych, lub innych czynności w ramach regulowanej ustawą działalności objętej nadzorem Komisji, organu nadzoru państwa członkowskiego lub organu nadzoru państwa trzeciego, jak również dotyczącą czynności podejmowanych w ramach wykonywania tego nadzoru.

Podobnie na rynku kapitałowym tajemnica zawodowa jest zdefiniowana w art. 147 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi[13], zgodnie z którym tajemnica zawodowa obejmuje informację uzyskaną w związku z podejmowanymi czynnościami służbowymi w ramach pozostawania w stosunku pracy, zlecenia lub w innym stosunku prawnym o podobnym charakterze, dotyczącą chronionych prawem interesów podmiotów dokonujących czynności związanych z obrotem instrumentami finansowymi, lub innych czynności w ramach regulowanej ustawą działalności objętej nadzorem Komisji lub zagranicznego organu nadzoru, jak również dotyczącą czynności podejmowanych w ramach wykonywania tego nadzoru, w szczególności informację zawierającą: 1) dane identyfikujące stronę umowy lub innej czynności prawnej; 2) treść umowy lub przedmiot czynności prawnej; 3) dane o sytuacji majątkowej strony umowy, w tym oznaczenie rachunku papierów wartościowych, innego rachunku, na którym zapisywane są instrumenty finansowe niebędące papierami wartościowymi, lub rachunku pieniężnego służącego do obsługi tych rachunków, liczbę i oznaczenie instrumentów finansowych, oraz wartość środków zgromadzonych na tych rachunkach; 4) oznaczenie rachunku zbiorczego, liczbę i oznaczenie zapisanych na nim instrumentów finansowych oraz dane osób uprawnionych z tych instrumentów finansowych.

Natomiast w ustawie z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych[14] w art. 49 ust. 2 zakres tajemnicy zawodowej określono w następujący sposób: tajemnica zawodowa, obejmuje informacje związane z lokatami funduszu, rejestrem członków funduszu, rozporządzeniami członków funduszu na wypadek śmierci oraz oświadczeniami, o których mowa w art. 83 tej ustawy (oświadczenia o stosunkach majątkowych), których ujawnienie mogłoby naruszyć interes członków funduszu lub interes

13 T.j. Dz.U. z 2020 r., poz. 89 ze zm.
14 T.j. Dz.U. z 2020 r., poz. 105 ze zm.

uczestników obrotu na rynku regulowanym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.

W przypadku dostawców usług płatniczych tajemnica zawodowa została określona w art. 11 ust. 3 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[15] i obejmuje informacje dotyczące użytkownika lub posiadacza pieniądza elektronicznego w związku ze świadczonymi mu usługami płatniczymi, wydawanym mu pieniądzem elektronicznym lub udzielonym mu kredytem w tym oznaczenie rachunku płatniczego użytkownika oraz stan tego rachunku, a także inne informacje związane z transakcjami płatniczymi oraz zawieranymi z użytkownikiem lub posiadaczem pieniądza elektronicznego umowami, jeżeli nieuprawnione ujawnienie takiej informacji mogłoby narazić na szkodę prawnie chroniony interes użytkownika lub posiadacza pieniądza elektronicznego, którego ta informacja dotyczy.

Z porównania tych regulacji wynika, że co do zasady chronią one informacje o kliencie instytucji finansowych związanych z zawieranymi przez niego transakcjami czy czynnościami, w których uczestniczy, a w szczególności wszelkie informacje dotyczące stanu majątkowego klienta instytucji finansowej. Dostęp do informacji i obowiązek przestrzegania tak określonej tajemnicy zazwyczaj mają wszystkie osoby działające w imieniu instytucji finansowej bez względu na formę i typ stosunku prawnego łączącego je z tymi instytucjami[16] i obowiązek ten nie wygasa także po ustaniu stosunku prawnego danej osoby z instytucją finansową[17]. Zasady udostępnienia informacji objętych tak określoną tajemnicą zawodową są ściśle określone[18], a w instytucjach, które są uprawnione do ich pozyskania objęte są one stosowną ochroną[19]. Instytucje finansowe obowiązane są jednak także do zawiadamiania właściwych organów ścigania w przypadku uzasadnionego podejrzenia wykorzystania ich

15 T.j. Dz.U. z 2019 r., poz. 659 ze zm.

16 Por. art. 11 ust. 1 ustawy o usługach płatniczych, odmiennie w art. 9e ust. 2 ustawy o spółdzielczych kasach oszczędnościowo-kredytowych, gdzie dostęp do tajemnicy zawodowej ograniczony jest do członków organów kasy i osób pozostających z nią w stosunku pracy.

17 Por. art. 11 ust. 2 ustawy o usługach płatniczych, art. 9e ust. 3 ustawy o spółdzielczych kasach oszczędnościowo-kredytowych.

18 Por. np. art. 105 Prawa bankowego, art. 9f ustawy o spółdzielczych kasach oszczędnościowo-kredytowych, art. 12 ustawy o usługach płatniczych, art. 35 ust. 2 ustawy o działalności ubezpieczeniowej i reasekuracyjnej.

19 Por. np. art. 16 ustawy o nadzorze nad rynkiem finansowym.

działalności w celu ukrycia działań przestępczych itp i działalności takiej nie chroni tajemnica[20].

Podkreślić należy, że Prawo bankowe w art. 105a wprowadziło szczególne zasady przetwarzania przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów (w Polsce są to przede wszystkim spółdzielcze kasy oszczędnościowo-kredytowe), instytucje pożyczkowe (w tym z innych państw), a także biura informacji kredytowej informacji stanowiących tajemnicę bankową, które umożliwiają m.in. profilowanie ich klientów w oparciu o te informacje.

W przypadku, gdy ustawodawca dopuszcza korzystanie przez instytucje finansowe z outsourcingu[21], wprowadza też stosowne uregulowania pozwalające na dostęp podmiotów świadczących takie usługi także do informacji objętych tajemnicą[22].

Zazwyczaj informacje stanowiące tajemnicę zawodową (w tym bankową) są przetwarzane w formie elektronicznej, zwłaszcza, że w szeregu przypadków ustawodawca wprost przewiduje możliwość składania oświadczeń woli związanych z czynnościami i usługami świadczonymi przez instytucje finansowe w postaci elektronicznej[23]. Oznacza to, że ochrona informacji stanowiących tajemnicę zawodową (w tym tajemnicę bankową) w instytucjach finansowych obejmuje także ochronę ich systemów teleinformatycznych i stosowanych przez nie systemów przetwarzania danych.

Zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[24] cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. A zatem zabezpieczenie informacji stanowiących tajemnicę zawodową w instytucjach finansowych stanowi element cyberbezpieczeństwa.

20 Por. art. 106a Prawa bankowego, art. 35 ust. 6 ustawy o działalności ubezpieczeniowej i reasekuracyjnej.

21 Por. np. art. 6a–6e Prawa bankowego, art. 9a–9d ustawy o spółdzielczych kasach oszczędnościowo-kredytowych.

22 Por. np. art. 104 ust. 2 pkt 2 Prawa bankowego, art. 9f ust. 1 pkt 2 ustawy o spółdzielczych kasach oszczędnościowo-kredytowych, art. 35 ust. 2 pkt 26 ustawy o działalności ubezpieczeniowej i reasekuracyjnej.

23 Por. art. 7b Prawa bankowego, art. 3a ustawy o spółdzielczych kasach oszczędnościowo-kredytowych.

24 Dz.U. z 2018 r., poz. 1560 ze zm.

Zgodnie z art. 4 pkt 9 i 10 ustawy o krajowym systemie cyberbezpieczeństwa, krajowy system cyberbezpieczeństwa obejmuje bank centralny (Narodowy Bank Polski) i jedyny obecnie działający w Polsce bank państwowy (Bank Gospodarstwa Krajowego).

Do usług kluczowych zaliczono przyjmowanie przez instytucje kredytowe depozytów pieniężnych lub innych funduszy podlegających zwrotowi od klientów; udzielanie kredytów na swój własny rachunek; wykonywanie przez bank następujących czynności: przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów lub prowadzenie innych rachunków bankowych, lub udzielanie kredytów, lub przeprowadzanie bankowych rozliczeń pieniężnych, lub udzielanie pożyczek pieniężnych, lub świadczenie usług płatniczych oraz wydawanie pieniądza elektronicznego, lub terminowe operacje finansowe, lub nabywanie i zbywanie wierzytelności pieniężnych, lub wykonywanie czynności zleconych, związanych z emisją papierów wartościowych, lub dokonywanie obrotu papierami wartościowymi, lub świadczenie usług zaufania oraz wydawanie środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania, lub przyjmowanie wpłat gotówki i dokonywanie wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku, lub 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, przy użyciu karty płatniczej lub podobnego instrumentu płatniczego, przez wykonywanie usług polecenia przelewu, w tym stałych zleceń, lub 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 dnia 19 sierpnia 2011 r. o usługach płatniczych, lub wydawanie instrumentów płatniczych, lub 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 świadczenie usługi inicjowania transakcji płatniczej; wykonywanie przez oddział banku

zagranicznego następujących czynności: przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów lub prowadzenie innych rachunków bankowych, lub udzielanie kredytów, lub przeprowadzanie bankowych rozliczeń pieniężnych, lub udzielanie pożyczek pieniężnych, lub świadczenie usług płatniczych oraz wydawanie pieniądza elektronicznego, lub terminowe operacje finansowe, lub nabywanie i zbywanie wierzytelności pieniężnych, lub wykonywanie czynności zleconych, związanych z emisją papierów wartościowych, lub dokonywanie obrotu papierami wartościowymi, lub świadczenie usług zaufania oraz wydawanie środków identyfikacji elektronicznej w rozumieniu przepisów o usługach zaufania, lub przyjmowanie wpłat gotówki i dokonywanie wypłat gotówki z rachunku płatniczego oraz wszelkie działania niezbędne do prowadzenia rachunku, lub wykonywanie transakcji płatniczych, w tym transferu środków pieniężnych na rachunek płatniczy u dostawcy użytkownika lub u innego dostawcy: przez wykonywanie usług polecenia zapłaty, w tym jednorazowych poleceń zapłaty, przy użyciu karty płatniczej lub podobnego instrumentu płatniczego, przez wykonywanie usług polecenia przelewu, w tym stałych zleceń, lub 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 dnia 19 sierpnia 2011 r. o usługach płatniczych, lub wydawanie instrumentów płatniczych, lub 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 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 ustawy – Prawo bankowe, wykonywanie czynności, o których mowa w art. 3 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych w zakresie określonym w tym przepisie; prowadzenie 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); prowadzenie rozliczeń i transakcji zawieranych w obrocie instrumentami finansowymi[25].

Zgodnie z załącznikiem nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa instytucjami finansowymi, które w trybie art. 5 tej ustawy mogą być uznane za operatora usługi kluczowej w drodze decyzji o uznaniu za operatora usługi kluczowej mogą być instytucje kredytowe, banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, spółdzielcze kasy oszczędnościowo-kredytowe, podmiot prowadzący rynek regulowany na podstawie ustawy o obrocie instrumentami finansowymi, 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[26]), spółka, której Krajowy Depozyt Papierów Wartościowych przekazał wykonywanie określonych zadań.

W konsekwencji należy uznać, że nie wszystkie czynności i usługi świadczone przez instytucje finansowe zostały uznane za usługi kluczowe, a także nie wszystkie instytucje finansowe mogą być uznane za operatorów usług kluczowych stanowiących część krajowego systemu cyberbezpieczeństwa. Zatem nie na wszystkie instytucje finansowe nałożono obowiązki określone w art. 8–16 ustawy o krajowym systemie cyberbezpieczeństwa. W przypadku, gdy instytucje finansowe korzystają z internetowej platformy handlowej rozumianej jako 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[27] traktowane będą jak dostawcy usługi cyfrowej[28], co wiązać się będzie z nałożeniem

25 Załącznik do rozporządzenia Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz.U. z 2018 r., poz. 1806).

26 Art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. UE L.2012.201.1 ze zm.).

27 Załącznik nr 2 do ustawy o krajowym systemie cyberbezpieczeństwa.

28 Na nieprecyzyjność zawartej w załączniku nr 2 do ustawy o krajowym systemie cyberbezpieczeństwa wskazuje M. Siwicki, *Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „Europejski

na nich obowiązków określonych w art. 17–20 ustawy o krajowym systemie cyberbezpieczeństwa. Na Narodowym Banku Polskim i Banku Gospodarstwa Krajowego jako podmiotach publicznych, o których mowa w art. 4 pkt 9 i 10 ustawy o krajowym systemie cyberbezpieczeństwa ciążą obowiązki określone w art. 21–25 tej ustawy.

O ile zatem tajemnica zawodowa w instytucjach finansowych, co do zasady nie zależy od rodzaju usługi lub czynności świadczonej przez tę instytucję, to zakres obowiązków związanych z incydentami w zakresie cyberbezpieczeństwa dotyczącymi naruszenia poufności danych chronionych taką tajemnicą objęty jest zróżnicowaną regulacją ustawy o krajowym systemie cyberbezpieczeństwa w zależności zarówno od instytucji finansowej i jej typu, jak i rodzaju usługi lub czynności, z którą związana była tajemnica zawodowa. Mimo to należy uznać, że regulacja rangi ustawowej nakładająca na poszczególne instytucje finansowe uznane za dostawców usług kluczowych obowiązki związane z cyberbezpieczeństwem, szacowaniem ryzyka, wdrożenia odpowiednich środków technicznych i organizacyjnych, zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty, zarządzanie incydentami i zapobieganie i ograniczanie wpływu incydentów na bezpieczeństwo systemu informacyjnego, a także audytami bezpieczeństwa systemów informacyjnych[29] powinna wpływać na bezpieczeństwo danych chronionych tajemnicą zawodową, także jeżeli są przetwarzane z wykorzystaniem systemów informatycznych przez instytucje finansowe. W stosunku do części instytucji finansowych Komisja Nadzoru Finansowego wydała także stosowne rekomendacje[30] i wytyczne[31]. Do banków zastosowanie ma Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska

Przegląd Sądowy" 2019, nr 9, s. 15–17 oraz M. Kruk, *Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom*, „Prawo Mediów Elektronicznych" 2019, nr 1, s. 29.

29 Por. art. 8 i 15 ustawy o krajowym systemie cyberbezpieczeństwa.

30 O roli rekomendacji nadzorczych w działalności Komisji Nadzoru Finansowego – A. Jakubiak, *Rekomendacja nadzorcza w kontekście regulacji polskich i europejskich* [w:] W. Rogowski (red.), *Polityka i praktyka regulacji rynków finansowych*, Kraków–Warszawa 2015. O roli rekomendacji i wytycznych – Z. Ofiarski, *Rola soft law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego* [w:] A. Jurkowska-Zeidler, M. Olszak (red.), *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Warszawa 2016, s. 137–160.

31 Por. C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo*, Warszawa 2020, s. 28–31; C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 339–361.

teleinformatycznego w bankach[32], zawierająca m.in. rekomendacje w zakresie zarządzania bezpieczeństwem środowiska teleinformatycznego, a do spółdzielczych kas oszczędnościowo-kredytowych Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych[33]. Komisja Nadzoru Finansowego wydała także Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych[34], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji[35], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych[36], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji[37], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w podmiotach infrastruktury rynku kapitałowego[38], Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych[39], których w każdym przypadku częścią są m.in. wytyczne w zakresie zarządzania bezpieczeństwem środowiska teleinformatycznego. Ponadto Komisja Nadzoru Finansowego wydała Rekomendację dotyczącą bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego

32 https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf.
33 https://www.knf.gov.pl/knf/pl/komponenty/img/Reko_SKOK_D_47953.pdf.
34 https://www.knf.gov.pl/knf/pl/komponenty/img/knf_125701_PTE_Wytyczne_IT_16_12_2014_40005.pdf.
35 https://www.knf.gov.pl/knf/pl/komponenty/img/ZU_Wytyczne_IT_16_12_2014_40004.pdf.
36 https://www.knf.gov.pl/knf/pl/komponenty/img/Wytyczne_IT_TFI_39999.pdf.
37 https://www.knf.gov.pl/knf/pl/komponenty/img/ZU_Wytyczne_IT_16_12_2014_40004.pdf.
38 https://www.knf.gov.pl/knf/pl/komponenty/img/Wytyczne%20_IT_infrastruktura_40003.pdf.
39 https://www.knf.gov.pl/knf/pl/komponenty/img/wytyczne_IT_firmy_inwestycyjne_40002.pdf.

i spółdzielcze kasy oszczędnościowo-kredytowe[40], wskazując w niej m.in. zagrożenia w zakresie bezpieczeństwa i ochrony danych użytkowników[41].

Zarówno regulacje prawne, jak i działania właściwych organów państwowych mają na celu zwiększenie zaufania do działających w Polsce instytucji finansowych także w zakresie przetwarzanych przez nie informacji dotyczących ich klientów i dokonywanych przez nich czynności i usług, z których korzystają, tak by zapewnić mechanizmy ochrony posiadanych przez instytucje finansowe informacji dotyczących ich klientów, niezależnie od ochrony mającej zastosowanie do danych osobowych, także jeżeli są przetwarzane przez instytucje finansowe. Podkreślić należy, że nawet jeżeli celem poszczególnych regulacji i rozwiązań nie jest wprost ochrona tajemnicy zawodowej, to jednak służą także tej ochronie. Ochrona tajemnicy zawodowej nie jest jednak bezwzględna, a informacje nią chronione mogą trafiać do innych podmiotów uprawnionych do ich otrzymania od instytucji finansowych (właściwe instytucje publiczne, inne instytucje finansowe, outsourcerzy, doradcy prawni itp.). Choć zatem ochrona poufności jest jednym z elementów cyberbezpieczeństwa, to charakter regulacji dotyczących cyberbezpieczeństwa i ochrony informacji objętych tajemnicą zawodową w instytucjach finansowych jest odmienny ze względu na stawiane im cele. Mimo to regulacje te mogą ułatwiać osiąganie dóbr chronionych – zarówno w zakresie cyberbezpieczeństwa, jak i tajemnicy zawodowej w tym tajemnicy bankowej, a dodatkowym elementem wpływającym pozytywnie w tym zakresie mogą być odrębne regulacje w zakresie ochrony danych osobowych[42] wprowadzone na poziomie europejskim, których adresatami są także instytucje finansowe.

Zwiększenie bezpieczeństwa systemów informacyjnych instytucji finansowych oraz poziomu ochrony danych osobowych niewątpliwie pozytywnie wpływa zatem na poziom ochrony tajemnicy zawodowej przez te instytucje i jest jednym z czynników zwiększających bezpieczeństwo ich funkcjonowania.

40 https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_43526.pdf.

41 Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe, s. 2.

42 Por. C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo…*, s. 31–32, 52–57, 109–111; C. Banasiński (red.), *Cyberbezpieczeństwo…*, s. 381–432; W. Hydzik, *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Przegląd Ustawodawstwa Gospodarczego" 2019, nr 3, s. 84–87.

Bibliografia

Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.
Banasiński C., Rojszczak M. (red.), *Cyberbezpieczeństwo*, Warszawa 2020.
Byrski J., Sytniewski L., *Zmiany w praktyce działania instytucji finansowych na skutek ogólnego rozporządzenia o ochronie danych. Wybrane zagadnienia prawne* [w:] W. Rogowski (red.), *Regulacje Finansowe. FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017.
Byrski J., *Tajemnica prawnie chroniona w działalności bankowej*, Legalis 2010.
Hydzik W., *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Przegląd Ustawodawstwa Gospodarczego" 2019, nr 3.
Iwanicz-Drozdowska M. (red.), *Kryzysy bankowe. Przyczyny i rozwiązania*, Warszawa 2002.
Jakubiak A., *Rekomendacja nadzorcza w kontekście regulacji polskich i europejskich* [w:] W. Rogowski (red.), *Polityka i praktyka regulacji rynków finansowych*, Kraków–Warszawa 2015.
Kruk M., *Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom*, „Prawo Mediów Elektronicznych" 2019, nr 1.
Krzysztofek M., *Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych*, LEX 2015.
Obal T., *System gwarantowania depozytów w USA* [w:] W. Baka (red.), *Systemy gwarantowania depozytów w Polsce i na świecie. Dziesięć lat Bankowego Funduszu Gwarancyjnego*, Warszawa 2005.
Ofiarski Z., *Rola soft law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego* [w:] A. Jurkowska-Zeidler, M. Olszak (red.), *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, Warszawa 2016.
Siwicki M., *Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „Europejski Przegląd Sądowy" 2019, nr 9.
Stępień K., *Instytucje Sieci Bezpieczeństwa Finansowego w Polsce z perspektywy instrumentów zapewniających stabilność finansową*, „Roczniki Ekonomii i Zarządzania" 2017, nr 3.

A professional secrecy in financial market institutions in the context of Polish cybersecurity regulations

Abstract

Financial market regulations contain regulations on professional secrecy, including banking secrecy, while there is no uniform regulation – for each type of financial institution the regulation in this respect is separate. Professional secrecy is not absolute, however, and the legislator sets out the rules for its sharing and exchange with other entities. Some financial institutions may be operators of key services under the national cybersecurity system, some may be treated as providers of digital services, and two of them – National Bank of Poland and the National Economy Bank (Bank Gospodarstwa Krajowego) are public entities that are part of the national cybersecurity system. Confidentiality is also an element of cybersecurity, so when processing information that is a professional secrecy in information systems, the regulations regarding the national cybersecurity system may also apply. Despite the same objectives, the application of regulations on professional secrecy and regulations on cybersecurity can be mutually reinforcing, which can be additionally supported by the application of separate regulations adopted at European level in the field of personal data protection.

Key words: cybersecurity, professional secrecy, banking secrecy, financial institution, financial market