Dariusz Gradzi

Third Party Providers (TPP)[1] – nowi dostawcy usług płatniczych w środowisku internetowym i mobilnym. Przegląd regulacji prawnych i analiza możliwych zagrożeń cyberbezpieczeństwa płatniczej infrastruktury krytycznej

Uwagi wstępne

Dyrektywa w sprawie usług płatniczych (dalej: dyrektywa PSD I)[2] wprowadziła do europejskiego porządku prawnego pojęcia usługi płatnicze, zamknięty katalog usług płatniczych, a także podmioty mogące świadczyć usługi płatnicze (tzw. dostawcy). Od czasu jej wejścia w życie na rynku rozwinęły się nowe płatnicze usługi elektroniczne realizowane z wykorystaniem infrastruktury internetowej, w tym szczególnie usługi oparte na dostępie do rachunków płatniczych (m.in. bankowych) podmiotów trzecich, którym takie uprawnienie przyznał posiadacz (użytkownik) rachunku (np. klient banku).

Wśród płatności elektronicznych wyróżnia się płatności internetowe[3] oraz płatności mobilne[4]. Mogą one być przeprowadzane między innymi jako płatności przy użyciu karty płatniczej oraz poleceń przelewu (tradycyjny przelew bankowy lub tzw. *pay-by-link*[5] – PBL). Rozwój handlu w środowisku interne-

[1] Ang. *Third Party Payment Service Provider* – dostawca usług płatniczych będący podmiotem trzecim. Zob. M. Mostowik, *Prawna ochrona informacji o rachunku płatniczym w świetle usługi dostępu do informacji o rachunku (AIS)*, „Monitor Prawa Bankowego" 2017, nr 7–8, s. 32.

[2] *Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48 WE i uchylająca dyrektywę 97/5/WE* (Dz. Urz. UE L 319 z 5 grudnia 2007 r., s. 1).

[3] B. Chinowski, *Elektroniczne metody płatności. Istota, rozwój, prognozy*, https://www.knf.gov.pl/knf/pl/komponenty/img/Elektroniczne%20metody%20platnosci.pdf, s. 5 [dostęp: 20 X 2017].

[4] Są to płatności dokonywane przy użyciu mobilnego urządzenia wyposażonego w system operacyjny, z multimedialnym interfejsem z wykorzystaniem technologii radiowej, sieci telekomunikacyjnych bezprzewodowych (GSM, GPRS, UMTS, Wi-Fi, NFC, RFiD, Bluetooth), *Final recommendations for the security of payment account access services following the public consultation*, Europejski Bank Centralny, https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf [dostęp: 25 X 2017].

[5] Jest to metoda płatności internetowej polegająca na tym, że podczas zakupów online, przy dokonywaniu płatności przez „bramkę płatniczą", klient otrzymuje specjalny link, który przekierowuje go do banku prowadzącego jego rachunek. Po zalogowaniu się do systemu bankowości elektronicznej pojawia się uzupełniony format przelewu z danymi odbiorcy (przeważnie agenta rozliczeniowego) oraz kwotą. Po autoryzacji przelewu odbiorca dostaje komunikat o wykonaniu płatności i może przystąpić do wykonania umowy, co znacznie przyspiesza transakcje online. Warunkiem skorzystania przez płatnika z tej usługi jest jej udostępnianie przez bank, w którym płatnik ma rachunek. Por. M. Grabowski, *Instrumenty płatnicze w prawie polskim*, https://depotuw.ceon.pl/bitstream/handle/item/327/Instrumenty%20Płatnicze%20w%20prawie%20polskim.pdf?sequence=1, s. 211 [dostęp: 4 X 2017].

towym oraz konieczność przyspieszenia realizacji procesu płatności spowodował ewolucję usług inicjujących płatność przez wprowadzenie interfejsu (tzw. bramki płatniczej, ang. *payment gate*) łączącego stronę internetową akceptanta (np. sklepu) ze stroną dostawcy usług płatniczych (np. banku)[6]. Dodatkowo poza usługami płatniczymi mającymi na celu dokonanie płatności pomiędzy płatnikiem a odbiorcą środków (lub podmiotem działającym na podstawie umowy z nim zawartej, np. agentem rozliczeniowym) pojawiły się nowe usługi uzupełniające, o których będzie mowa w niniejszym artykule. Do nowych usług uzupełniających wprowadzonych drugą dyrektywą w sprawie usług płatniczych (dalej: dyrektywa PSD II)[7] należą:

– usługa inicjacji płatności przez podmiot trzeci,
– usługa dostępu do informacji o rachunku przez podmiot trzeci,
– potwierdzenie dostępności środków pieniężnych na rachunku płatniczym[8].

Powyższe usługi zapewniają użytkownikowi możliwość przyspieszenia transakcji płatniczej oraz dostęp do zagregowanych[9] informacji o rachunku płatniczym online, udostępnianych przez interfejs dostawcy prowadzącego rachunek płatniczy. Dzięki tej ostatniej usłudze użytkownik ma możliwość szybkiego zorientowania się w swojej sytuacji finansowej[10].

Przedmiotem niniejszego artykułu będzie prezentacja nowych usług płatniczych wprowadzonych do europejskiego, i tym samym – polskiego, porządku prawnego przez dyrektywę PSD II oraz zagrożeń w skali mikro i makro, jakie mogą się wiązać z ich funkcjonowaniem. Fundamentem regulacji zawartych w dyrektywie PSD II jest przyznanie płatnikom prawa do korzystania z usług podmiotów trzecich oraz konieczność respektowania tego prawa przez dostawcę prowadzącego rachunek płatniczy (w tym bankowy) – tzw. *Account Servicing Payment Service Provider* (ASPSP). W dyrektywie PSD II przewidziano odpowiednie mechanizmy[11] prawne przełamujące ewentualny brak woli współpracy ze strony ASPSP z TPP[12]. Dostawcy prowadzący rachunek płatniczy zostali zatem zmuszeni prawnie do współpracy z TPP.

---

[6] Por. motyw 27 do preambuły dyrektywy PSD II.

[7] *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) 1093/2010 oraz uchylająca dyrektywę 2007/64/WE* (Dz. Urz. UE L 337 z 23 grudnia 2015 r., s. 35).

[8] W przeciwieństwie do usługi inicjacji płatności oraz usługi dostępu do informacji o rachunku potwierdzanie dostępności środków pieniężnych na rachunku nie jest odrębną usługą płatniczą. Por. K. Korus, *Usługi oparte na dostępie do rachunku w dyrektywie PSD II*, „Monitor Prawa Bankowego" 2017, nr 7–8, s. 85.

[9] Informacja zagregowana to wszelka informacja odnosząca się do wieloelementowych zbiorów obiektów jednostkowych lub wieloelementowych zbiorów cech tych obiektów, za: J. Oleński, *Ekonomika informacji. Podstawy*, Warszawa 2001, s. 209 (przyp. red.).

[10] Motyw 28 do preambuły dyrektywy PSD II.

[11] Są nimi: sankcje ze strony organu nadzoru – KNF, a także obowiązek notyfikacji wynikający z art. 68 ust. 6 dyrektywy PSD II.

[12] Należy zauważyć, że w ujęciu biznesowym TPP są bezpośrednią konkurencją dla ASPSP.

W obecnych realiach rynkowych ASPSP często uniemożliwiają rozwój TPP przez: blokowanie określonych adresów IP[13] tych dostawców, blokowanie rachunku bankowego płatnika[14] lub uniemożliwianie tzw. *screen scrapingu*[15].

Dane statystyczne i zagrożenia

Cechą wspólną usług TPP jest to, że w celu ich wykonania jest niezbędne uzyskanie przez podmiot trzeci dostępu do rachunku płatniczego (bankowego). Tego typu usługi do tej pory nie doczekały się regulacji prawnej, choć są realizowane na rynku finansowym od wielu lat. Powodem takiego stanu rzeczy było to, że w przypadku tych usług nie dochodzi do wejścia przez TPP w posiadanie środków pieniężnych[16]. A zatem ci dostawcy mogli korzystać z wyłączenia stosowania przepisów dyrektywy PSD I oraz ustawy o usługach płatniczych[17] (dalej: UUP) w brzmieniu przed implementacją do polskiego porządku prawnego dyrektywy PSD II[18]. Dyrektywa PSD II przyniosła zmiany w postaci konieczności – co do zasady – uzyskania zezwolenia organu nadzoru (w Polsce – Komisji Nadzoru Finansowego) na świadczenie tych usług.

Usługi TPP mają prowadzić do ułatwienia i przyspieszenia płatności w środowisku internetowym. Należy jednak zwrócić uwagę na możliwe zagrożenia, jakie będą się wiązały z pojawieniem się nowych usług oraz nowych dostawców. Według danych statystycznych liczba wykrytych cyberataków na firmy w Polsce w 2015 r. w stosunku do 2014 r. wzrosła o 46 proc. Największym czynnikiem ryzyka dla sektora finansowego jest zagrożenie atakami na systemy IT[19]. W 2014 r. w w naszym kraju około 230 tys. komputerów miało zainstalowane złośliwe oprogramowanie, z czego aż 50 tys. przypadków dotyczyło złośliwego oprogramowania w postaci trojana bankowego[20]. Liczba użytkowników bankowości mobilnej przez ostatnie cztery lata

[13] Ang. *Internet Protocol* (IP), zob. http://munitus.pl/co-to-jest-ip.html [dostęp: 4 X 2017].

[14] Zob. M. Mostowik, *Prawna ochrona informacji o rachunku*…, s. 33.

[15] Ang. s*creen scraping* – metoda dostępu do bankowości elektronicznej użytkownika polegająca na tym, że klient upoważnia bank (np. ten, w którym ubiega się o kredyt) do zalogowania się do jego rachunku płatniczego w innym banku (gdzie użytkownik posiada historię płatniczą) na skutek przekazania pierwszemu bankowi danych do logowania. Logowanie następuje przez analizę treści interfejsu bankowego za pośrednictwem systemu informatycznego pierwszego banku, który automatycznie dokonuje wprowadzenia loginu i hasła klienta w określone pola. Dalej następuje zalogowanie się do systemu bankowości elektronicznej. Zob. ostrzeżenie wydane przez KNF 14 VII 2014 r. pt. *Ryzyko związane z podawaniem innemu bankowi danych do logowania do rachunku bankowego*, https://www.knf.gov.pl/?articleId=53072&p_id=18 [dostęp: 23 X 2017].

[16] Art. 6 pkt 10 UUP w zw. z art. 3 lit. 1 dyrektywy PSD I.

[17] *Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych* (t.j.: Dz.U. z 2017 r. poz. 2003, ze zm.).

[18] Co nastąpiło *Ustawą z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw* (Dz.U. z 2018 r. poz. 1075).

[19] Ang. *Information Technology*, https://pl.wikipedia.org/wiki/Technologia_informacyjna [dostęp: 15 VIII 2018].

[20] Por. A. Marciniak, *Bankowy CERT – nowa broń w walce z cyberprzestępczością*, w: *Wyzwania informatyki bankowej 2016*, A. Kawiński, A. Sieradz (red.), Gdańsk 2016, s. 181–182.

wzrosła do około 8,2 mln (wzrost o 680 proc.)[21]. Sam zaś udział w tej liczbie właścicieli smartfonów korzystających z bankowości mobilnej wynosił w 2013 r. 12 proc., a w 2015 r. – 43 proc. [22]

Liczba transakcji bezgotówkowych zwiększa się każdego roku średnio o 15 proc. Kwotowo liczba poleceń przelewów wzrosła z 31 bln zł w 2010 r. do 47,5 bln zł w 2015 r. Udział poleceń przelewu w 2015 r. w odniesieniu do wszystkich transakcji bezgotówkowych wynosił 45 proc., natomiast liczba transakcji dokonywanych przy użyciu karty płatniczej w 2015 r. wyniosła 54 proc. (dla porównania 2010 r. – 36 proc.). Transakcje kartowe w latach 2009–2015 osiągnęły średnioroczny wzrost o 24 proc. [23] Liczba wydanych kart płatniczych w Polsce w 2014 r. to ponad 36 mln[24]. W 2013 r. udział kartowych transakcji oszukańczych w wartości wszystkich transakcji kartowych wyniósł 0,005 proc. [25]

Jednocześnie w latach 2005–2015 zwiększyła się liczba sieci akceptacji kart płatniczych (stanowiących tzw. POS[26], w których przypadku jest przyjmowana zapłata kartami płatniczymi) z 55 tys. punktów POS w 2005 r. do 184 tys. w 2015 r. Liczba pojedynczych terminali POS do akceptacji kart płatniczych wzrosła w tym okresie ze 129 tys. do 463 tys. Zwiększył się także odsetek Polaków aktywnie korzystających z konta bankowego przez Internet. W 2009 r. wynosił on 46 proc., podczas gdy w 2016 r. – 69 proc.[27] Liczba rachunków bankowych prowadzonych dla osób prywatnych przez banki, oddziały instytucji kredytowych oraz Spółdzielcze Kasy Oszczędnościowo-Kredytowe wzrosła z 44 mln w 2010 r. do 58 mln w 2015 r.[28]

W pierwszym kwartale 2017 r. w Internecie odnotowano ponad 15 tys. akceptantów[29] oraz 11,5 mln transakcji płatniczych. Wartość tych transakcji wyniosła 1,78 mld zł. Dziennie odnotowywano średnio ponad 128 tys. transakcji[30]. Powyższe dane statystyczne pokazują nieodwracalną tendencję wzrostową rynku płatności bezgotówkowych i elektronicznych transakcji płatniczych[31].

---

[21] Zob. raporty z badań przeprowadzonych przez portal PRNews.pl za IV kwartał 2012 r. i I kwartał 2017 r., https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-i-kw-2017-360755 [dostęp: 23 X 2017]; https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-iv-kw-2013-16158 [dostęp: 23 X 2017].

[22] Zob. A. Marciniak, *Bankowy CERT – nowa broń*…

[23] *Stan obrotu bezgotówkowego w Polsce*, https://www.mr.gov.pl/media/30118/Rozwoj_obrotu_bezgotowkowego_112016.pdf [dostęp: 10 X 2017].

[24] *Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2015 r.*, https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/porownanie_UE_2014.pdf, s. 18 [dostęp: 10 X 2017].

[25] Tamże, s. 31.

[26] Ang. *points of sale*.

[27] D. Maison, *Postawy Polaków wobec obrotu bezgotówkowego. Raport z badania 2016 i analiza porównawcza z danymi z 2009 i 2013 r.*, https://www.nbp.pl/badania/seminaria/8v2017.pdf [dostęp: 10 X 2017].

[28] *Porównanie wybranych elementów polskiego systemu płatniczego*…, s. 6.

[29] Akceptantem jest np. sklep internetowy.

[30] *Informacja o kartach płatniczych I kwartał 2017 r.*, https://www.nbp.pl/systemplatniczy/karty/q_01_2017.pdf, s. 36 [dostęp: 10 X 2017].

[31] *Stan obrotu bezgotówkowego w Polsce*…

Powyższe dane prowadzą do wniosku, że działalność TPP, zwłaszcza w początkowym okresie, powinna być szczególnie nadzorowana i weryfikowana, z uwagi na potencjalne zagrożenia tzw. ekosystemu finansowego, który jest oparty na wzajemnym zaufaniu jego uczestników i dbaniu o bezpieczeństwo użytkowników końcowych.

Usługi płatnicze oraz ich dostawcy – charakterystyka prawna

Przed dalszą analizą nowych usług płatniczych konieczne jest objaśnienie terminów, które pozwolą na zrozumienie procesu dokonywania płatności elektronicznej i zaprezentowanie jej uczestników. Zgodnie z polską ustawą o usługach płatniczych:

- dostawca – to podmiot świadczący usługi płatnicze. UUP zawiera zamknięty katalog dostawców, którymi mogą być m.in.: banki krajowe, instytucje kredytowe, instytucje pieniądza elektronicznego, instytucje płatnicze, spółdzielcze kasy oszczędnościowo-kredytowe oraz biura usług płatniczych, co oznacza, że inne podmioty nie mogą świadczyć tych usług pod rygorem odpowiedzialności karnej[32];
- akceptant – to odbiorca inny niż konsument, dla którego agent rozliczeniowy świadczy usługę płatniczą (np. sklep stacjonarny lub internetowy). Jest to podmiot przyjmujący zapłatę w formie bezgotówkowej[33];
- usługa płatnicza – to usługa, której istotą jest transfer środków, np. przelew bankowy, czyli środki z rachunku w jednym banku zostają zapisane na rachunku użytkownika w innym banku. Ta usługa zmierza do umożliwienia płatnikowi przekazania środków pieniężnych do odbiorcy. UUP wprowadza zamknięty katalog usług płatniczych;
- użytkownik – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, korzystająca z usług płatniczych jako płatnik lub odbiorca;
- płatnik – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, składająca zlecenie płatnicze prowadzące do obciążenia jej rachunku płatniczego lub dokonania wpłaty środków (podmiot dokonujący płatności);
- odbiorca – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, będąca odbiorcą środków pieniężnych stanowiących przedmiot transakcji płatniczej (podmiot otrzymujący płatność);
- zlecenie płatnicze – to oświadczenie płatnika lub odbiorcy skierowane do dostawcy, zawierające polecenie wykonania transakcji płatniczej[34]. Inicjuje ono transakcję płatniczą. Do jego złożenia może być użyty instrument płatniczy. Zlecenie, o którym mowa, powinno zawierać dane umożliwiające

[32] Art. 150 i nast. UUP.
[33] M. Pacak, *Usługi płatnicze. Komentarz*, Warszawa 2014, s. 181.
[34] Tamże, s. 182.

przeprowadzenie transakcji, takie jak: dane płatnika i odbiorcy, kwota transakcji, unikatowy identyfikator odbiorcy, np. numer rachunku bankowego IBAN (*International Bank Account Number*)[35];

– transakcja płatnicza – to wpłata, transfer lub wypłata środków pieniężnych zainicjowane przez płatnika lub odbiorcę. Transakcja płatnicza może być:
  • zainicjowana przez płatnika, np. polecenie przelewu (tradycyjny przelew bankowy), w którym płatnik przesyła do swojego dostawcy usług płatniczych polecenie dokonania transakcji[36],
  • zainicjowana przez odbiorcę, jeśli płatnik uprzednio udzielił odbiorcy zgody na zainicjowanie transakcji. W tym wypadku to odbiorca inicjuje transakcję płatniczą bez udziału płatnika (np. polecenie zapłaty[37]);
– instrument płatniczy – to urządzenie lub zbiór procedur uzgodniony przez użytkownika i dostawcę, wykorzystywane przez użytkownika do składania zleceń płatniczych. Są to m.in.:
  • zestawy procedur technicznych, np. bankowość elektroniczna[38],
  • przedmioty materialne, np. karty płatnicze – tzw. instrumenty transakcyjne[39];
– karta płatnicza[40] – to karta uprawniająca do wypłaty gotówki (bankomatowa) lub umożliwiająca złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego;
– karta debetowa – to karta płatnicza umożliwiająca wykonywanie transakcji płatniczych, z wyjątkiem transakcji w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu;
– karta kredytowa – to karta płatnicza umożliwiająca wykonywanie transakcji płatniczych w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu.

W świetle postanowień UUP w polskim porządku prawnym występują m.in. następujące usługi płatnicze:

– prowadzenie rachunku płatniczego (podmiotem uprawnionym do prowadzenia takiego rachunku są nie tylko banki), dokonywanie wypłat gotówki;
– przyjmowanie wpłat gotówki;
– wykonywanie transakcji płatniczych przy użyciu karty płatniczej lub podobnego instrumentu płatniczego;

---

[35] M. Grabowski, *Ustawa o usługach płatniczych. Komentarz*, Warszawa 2012, s. 28.

[36] Tamże, s. 27.

[37] Art. 63d *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* (t.j.: Dz.U. z 2017 r. poz. 1876, ze zm.).

[38] M. Grabowski, *Ustawa o usługach płatniczych*…, s. 19.

[39] K. Korus, *Pojęcie usługi płatniczej w ustawie o usługach płatniczych*, „Monitor Prawa Bankowego" 2012, nr 7–8, s. 37.

[40] Należy odnotować, że zagadnienia dotyczące kart płatniczych są szczegółowo regulowane przez *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę* (Dz. Urz. UE L 123 z 19 maja 2015, s. 1).

- realizacja poleceń zapłaty;
- realizacja polecenia przelewu (tradycyjny przelew bankowy);
- wydawanie instrumentów płatniczych (np. kart płatniczych), tzw. *issuing*;
- *acquiring* – wykonywanie transakcji płatniczych zainicjowanych przez akceptanta lub za jego pośrednictwem instrumentem płatniczym płatnika, szczególnie autoryzacja wykonywanych transakcji, przesyłanie do wydawcy karty płatniczej lub systemów płatności zleceń płatniczych mających na celu przekazanie akceptantowi należnych mu środków[41]; wyjątkiem jest rozrachunek transakcji w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami[42]. Są to transakcje, w których np. jest dokonywana płatność kartą płatniczą w sklepie (u tzw. akceptanta karty); akceptant autoryzuje i rozlicza transakcję w ramach usług *acquiringu* świadczonych przez agentów rozliczeniowych, ci zaś przekazują zlecenie płatnicze do banku (czyli do wydawcy karty należącej do osoby dokonującej płatności) i po otrzymaniu z tego banku środków pieniężnych rozliczają się z akceptantem;
- świadczenie przekazu pieniężnego (transfer środków pieniężnych przyjętych od płatnika bez prowadzenia dla niego rachunku płatniczego do odbiorcy, np. przyjmowanie opłat za drobne rachunki w celu ich przekazania usługodawcom lub przyjmowanie wpłat w celu ich udostępnienia odbiorcy);
- świadczenie usługi inicjowania transakcji płatniczej;
- świadczenie usługi dostępu do informacji o rachunku[43].

Obszary infrastruktury płatniczej narażone na ryzyko

Należy wyróżnić następujące elementy[44] w obszarze infrastruktury płatności elektronicznych wrażliwe na zagrożenia:

- systemy płatności[45] podmiotów rozliczających transakcje płatnicze (np. Krajowa Izba Rozliczeniowa SA) oraz infrastruktury systemów kart płatniczych –

[41] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce*, Warszawa 2012, s. 107.

[42] *Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami* (t.j.: Dz.U. z 2018 r. poz. 145, ze zm.).

[43] Świadczenia: usługi inicjowania płatności oraz usługi dostępu do informacji o rachunku zostały dodane do UUP na podstawie dyrektywy PSD II ustawą o zmianie ustawy o usługach płatniczych.

[44] D. Gradzi, *Bezpieczeństwo płatności elektronicznych jako element cyberbezpieczeństwa państwa – przegląd regulacji prawnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 38.

[45] SORBNET2, TARGET2-NBP dla płatności wysokokwotowych, ELIXIR, EXPRESS ELIXIR, Krajowy System Rozliczeń, System płatności BlueCash, System Płatności Mobilnych BLIK, System Płatności Kartowych dla płatności detalicznych, http://www.nbp.pl/home.aspx?f=/systemplatniczy/nadzor_syst_platn/systemy_platnosci.html [dostęp: 15 X 2017].

schematów płatniczych (organizacji kartowych)[46],
- informatyczne systemy bankowe[47] oraz infrastruktura podmiotów zaangażowanych w procesowanie transakcji płatniczych (dostawców, w tym agentów rozliczeniowych),
- infrastruktura akceptantów, tj. podmiotów będących odbiorcami płatności elektronicznej[48],
- aplikacje i infrastruktura użytkowników końcowych, zarówno internetowych, jak i mobilnych (w tym urządzenia przenośne i komputery).

Część spośród powyższych elementów stanowi infrastrukturę krytyczną[49] objętą Narodowym Programem Ochrony Infrastruktury Krytycznej[50]. Te elementy należy sklasyfikować jako systemy finansowe, których funkcjonowanie jest możliwe dzięki systemom łączności i systemom teleinformatycznym.

Krytyczna infrastruktura państwa[51] obejmuje m.in. systemy bankowe i finansowe oraz telekomunikacyjne[52]. Składają się na nią rzeczywiste (obiekty, serwery) oraz cybernetyczne systemy, które tylko w przypadku współistnienia umożliwiają świadczenie usług płatniczych. Ze względu na specyfikę usług płatniczych (zdalny dostęp) oraz otwarty charakter systemów bankowych, do których wejście jest możliwe przy wykorzystaniu publicznych sieci, te systemy są narażone na cyberprzestępczość. Cyberprzestępczość jest rozumiana jako (…) *posługiwanie się sieciami telekomunikacyjnymi do naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne*[53]. W *Rządowym Programie Ochrony Cyberprzestrzeni RP na lata 2011–2016*[54] zdefiniowano cyberprzestępstwo jako (…) *czyn zabroniony popełniony w „cyberprzestrzeni"*. Cyberprzestrzeń jest definiowana w powyższym dokumencie jako

[46] Art. 2 ust. 19b) ustawy o usługach płatniczych definiuje organizację kartową jako podmiot określający zasady wydawania i akceptowania kart płatniczych, zawierający umowy z wydawcami (bankami) lub agentami rozliczeniowymi (będzie to np. VISA lub MasterCard).

[47] K. Radziejewski, *Cyberbezpieczeństwo w administracji rządowej w Rzeczpospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 313.

[48] Art. 2 ust. 1b) UUP definiuje akceptanta jako odbiorcę innego niż konsument, na którego rzecz agent rozliczeniowy świadczy usługę płatniczą – w tym ujęciu będzie to np. sklep internetowy akceptujący zarówno płatności kartowe, jak i płatności dokonywane za pośrednictwem tzw. *pay-by-linków*, czyli przelewów natychmiastowych, w ich przypadku kwota transakcji płatniczej jest rozliczna przy udziale pośredniczącego agenta rozliczeniowego.

[49] W rozumieniu art. 3 pkt. 2 ppkt. b), c) i d) *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (t.j.: Dz.U. z 2018 r. poz. 1401).

[50] W rozumieniu art. 5b) ustawy o zarządzaniu kryzysowym.

[51] Por. art. 3 pkt 2 ustawy o zarządzaniu kryzysowym.

[52] Por. tamże oraz R. Kośla, *Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac*, http://www.cert.pl/PDF/Kosla_p.pdf [dostęp: 2 X 2017].

[53] M. Staszczyk, *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, http://www.finanseiprawofinansowe.uni.lodz.pl/Publikacje/5/4_Staszczyk.pdf, s. 46 [dostęp: 2 X 2017].

[54] *Rządowy Program Ochrony Cyberprzestrzeni RP*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf, s. 6 [dostęp: 17 VIII 2018].

(…) *cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*. Statystyki incydentów w cyberprzestrzeni koordynowanych przez CERT[55] pokazują wzrost liczby tych incydentów w stosunku do lat poprzednich. W 2014 r. zarejestrowano ponad 12 tys. zgłoszeń, z czego 7,4 tys. zakwalifikowano jako rzeczywiste incydenty, w 2015 r. zaś zarejestrowano ponad 16 tys. zgłoszeń, a 8,9 tys. z nich zakwalifikowano jako tego typu incydenty[56].

Wystąpienie zagrożenia w powyższych obszarach infrastruktury krytycznej może być sklasyfikowane jako zdarzenie o charakterze terrorystycznym[57] implikujące wprowadzenie stopni alarmowych CRP[58] – w przypadku wystąpienia sytuacji, co do której istnieje podejrzenie, że powstała wskutek przestępstwa o charakterze terrorystycznym lub zagrożenia zaistnienia takiego przestępstwa[59]. Przestępstwem o charakterze terrorystycznym jest między innymi czyn zabroniony, zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej pięć lat, popełniony w celu wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczpospolitej Polskiej lub sama groźba popełnienia takiego czynu dotyczącego szczególnie infrastruktury krytycznej. Możliwe bowiem jest wykorzystanie bankowej infrastruktury krytycznej przez TPP i spowodowanie szkody majątkowej, której wysokości nie da się przewidzieć, zarówno bankom jak i ich klientom.

Third Party Providers – regulacje prawne

Aktami prawnymi regulującymi dostęp podmiotów trzecich do rachunków płatniczych są[60]:

- dyrektywa PSD II;
- *Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów*

[55] Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, http://www.cert.gov.pl/cer/o-nas/15,O-nas.html [dostęp: 10 X 2017]. W dniu 28 VIII 2018 r. CERT.GOV.PL przekształcił się w CSIIRT,GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (podstawa: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Dz.U. z 2018 r. poz. 1560) – dop. red.

[56] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html [dostęp: 3 X 2017].

[57] W rozumieniu art. 2 pkt. 7 *Ustawy z dnia 10 czerwca 2016 o działaniach antyterrorystycznych* (t.j.: Dz.U. z 2018 r. poz. 452, ze zm.).

[58] Zgodnie z art. 15 ust. 2 ustawy o działaniach antyterrorystycznych.

[59] W rozumieniu art. 115 par. 20 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: Dz.U. z 2017 r. poz. 2204, ze zm.).

[60] W opracowaniu uwzględniono zarówno akty prawne uchwalone, jak i pozostające na etapie prac legislacyjnych.

komunikacji (dalej: RTS)[61], regulujące sposób komunikacji pomiędzy TPP a ASPSP[62]. Zostało ono wydane na podstawie art. 98 ust. 4 zd. 2 dyrektywy PSD II w związku z art. 10–14 rozporządzenia (UE) nr 1093/2010 w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego)[63]. RTS nie wymaga implementacji do krajowego porządku prawnego[64], a państwa członkowskie UE mają zapewnić przymusowo jego stosowanie przez TPP i ASPSP, począwszy od pierwszego dnia po upływie 18 miesięcy od daty wejścia w życie RTS;
– UUP oraz ustawa o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw[65].

Wspólny zakres zastosowania dyrektywy PSD II do TPP

Podmioty trzecie działają obecnie na rynku usług płatniczych i są jego aktywnymi uczestnikami. Realizują wiele transakcji płatniczych o bardzo wysokiej wartości[66] (w 2014 r. z usług tylko jednego dostawcy TPP korzystało 8 mln osób w 11 krajach; od 2005 r. dostawca, o którym mowa, przeprowadził ponad 100 mln transakcji). Z tego powodu dyrektywa PSD II wprowadzała wymóg niedyskryminacji tych podmiotów

[61] Dz. Urz UE L 69 z 13 marca 2018 r., s. 23. Regulacyjne standardy techniczne są wydawane na podstawie art. 290 *Traktatu o funkcjonowaniu UE* – wersja skonsolidowana, Dz. Urz. C326/49 z 26 października 2012, s. 47) i stanowią tzw. drugi poziom w systemie aktów prawa UE. Opracowywane są m.in. przez European Banking Authority (EBA) – Europejski Urząd Nadzoru Bankowego – i jako projekt są przedkładane do Komisji Europejskiej. Komisja Europejska jest uprawniona do przyjmowania tzw. aktu nieustawodawczego o zasięgu ogólnym, który uzupełnia akt ustawodawczy (w niniejszym przykładzie – dyrektywę PSD II). RTS jest zatem wiążący dla krajów członkowskich lub instytucji nadzorowanych (np. banków). Komisja Europejska przedkłada RTS Radzie Unii Europejskiej oraz Parlamentowi Europejskiemu, które mogą dany akt odrzucić. Por. G. Włodarczyk, *Struktura i status aktów prawa Unii Europejskiej ze szczególnym uwzględnieniem RTS, ITS i tzw. Guidelines*, http://mifid.pl/wp-content/uploads/2015/11/Struktura-aktów-Unii-Europejskiej-ze-szczególnym-uwzględnieniem-RTS-ITS-i-tzw.-Guidelines.pdf, s. 4 [dostęp: 4 X 2017]; https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018R0389&from=EN [dostęp: 15 VIII 2018].

[62] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 [dostęp: 14 X 2017].

[63] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE* (Dz. Urz. UE L 331 z 15 grudnia 2010 r., s. 12).

[64] K. Korus, *Usługi oparte na dostępie*…, s. 82.

[65] Zob. ustawę o zmianie ustawy o usługach płatniczych.

[66] https://www.sofort.com/pol-PL/newsroom/prasowe/SOFORT-Banking-utrzmuje-szybkie-tempo-wzrostu [dostęp: 23 X 2017]; https://retailnet.pl/2015/06/22/13453-dagmara-kruszewska-sofort-3-mln-transakcji-miesiecznie/; http://prnews.pl/wiadomosci/sofort-wyniki-za-1-polowe-2016-50-sklepow-dziennie-chce-rozpoczac-wspolprace-6553123.html [dostęp: 14 X 2017].

do czasu implementacji jej przepisów[67]. Warto odnotować, że Komisja Nadzoru Finansowego w przeszłości wydawała ostrzeżenia przed działalnością TPP[68].

Dyrektywa PSD II wprowadza trzy rodzaje usług TPP określanych też jako usługi XS2A[69]. Są nimi:

- usługa inicjowania płatności (dalej: *Payment Initiation Service* albo – w przypadku podmiotu świadczącego taką usługę – podmiot ten jest zwany dalej: dostawcą usługi PIS) oznacza usługę inicjowania, na wniosek użytkownika, zlecenia płatniczego odnośnie do rachunku płatniczego posiadanego u innego dostawcy usług płatniczych[70]. Dostawca usługi PIS nie może wchodzić w żadnym momencie w posiadanie środków pieniężnych, co odróżnia tę formę płatności od tzw. przelewów natychmiastowych (ang. *pay-by-link*), w których „pośrednik" (agent rozliczeniowy) wchodzi w posiadanie tych środków;
- usługa dostępu do informacji o rachunku (dalej: *Account Information Service* albo – w przypadku podmiotu świadczącego taką usługę – podmiot ten jest zwany dalej: dostawcą usługi – AIS) oznacza usługę online, która polega na dostarczaniu kompletnych informacji na temat rachunku płatniczego posiadanego przez użytkownika usług płatniczych[71];
- potwierdzenie dostępności środków pieniężnych na rachunku płatniczym (*Confirmation of the Availability of Funds* albo – w przypadku podmiotu świadczącego taką usługę – podmiot ten jest zwany dalej: dostawcą usługi CAF), które nie stanowi osobnej usługi płatniczej i nie jest wymienione w załączniku nr 1 do dyrektywy PSD II.

Dostawca prowadzący rachunek płatniczy jest zobowiązany do zezwalania dostawcom usług PIS i AIS na poleganie na procedurach uwierzytelniania użytkowników zapewnianych przez ASPSP[72]. Powyższa regulacja prowadzi do wniosku, że TPP ma prawo do zastosowania własnego uwierzytelnienia użytkownika, niezależnie od uwierzytelnienia ASPSP, ale może także wykorzystać wyłącznie uwierzytelnienie użytkownika stosowane przez ASPSP.

Wszelkie prawne obowiązki nałożone przez dyrektywę PSD II na ASPSP mają zastosowanie wyłącznie wtedy, gdy ASPSP prowadzą dla użytkownika rachunek

---

[67] Motyw 29 i 33 do dyrektywy PSD II.

[68] Zob. *Ostrzeżenie KNF przed dopuszczeniem pośredników do rachunku bankowego w płatnościach internetowych z dnia 18.11.2013 r.* oraz *Ryzyko związane z podawaniem innemu bankowi danych do logowania do rachunku bankowego z dnia 14.07.2014 r.*, w: *Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe*, wydana przez KNF w listopadzie 2015 r., s. 2, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/Rekomendacja_dot_bezpieczenstwa_transakcji_platniczych [dostęp: 25 X 2017].

[69] Tzw. *access to account* (dostęp do rachunku), zob. M. Mostowik, *Prawna ochrona informacji o rachunku*…, s. 32.

[70] Art. 4 pkt 15 dyrektywy PSD II.

[71] Art. 4 pkt 16 dyrektywy PSD II.

[72] Art. 97 ust. 5 dyrektywt PSD II.

płatniczy. Rachunek bankowy jest rachunkiem płatniczym wówczas, gdy służy do wykonywania transakcji płatniczych[73]. Dostęp do informacji innych niż informacje o rachunku płatniczym (np. kredytach, lokatach, depozytach, inwestycjach) nie podlega regulacji dyrektywy PSD II[74].

Zakres stosowania dyrektywy PSD II dotyczy wyłącznie usług płatniczych świadczonych w Unii Europejskiej. Mankamentem takiego ujęcia jest to, że w przypadku, gdy działalność usługodawcy nie dotyczy krajów UE, to usługa TPP może być świadczona bez żadnych ograniczeń wynikających z dyrektywy PSD II, ale też bez możliwości domagania się przez TPP od ASPSP określonego zachowania, do którego ten podmiot jest zobowiązany na mocy przepisów wymienionej dyrektywy[75].

Obowiązki nałożone na ASPSP związane z dostępem do rachunków płatniczych przez TPP dotyczą wyłącznie sytuacji, gdy te rachunki są prowadzone przez ASPSP online. Dyrektywa PSD II nie definiuje, co należy rozumieć przez dostępność rachunku płatniczego online. Trafnie przyjmuje się, że ten termin należy rozumieć szeroko i obejmować nim przypadki każdej formy komunikacji za pośrednictwem systemów teleinformatycznych stron w czasie rzeczywistym[76].

Gwarancją możliwości świadczenia przez TPP usług, które są konkurencyjne i stoją w opozycji do interesów tzw. bankowych dostawców usług płatniczych, jest art. 36 dyrektywy PSD II. Przewiduje się w nim, że każda instytucja płatnicza powinna mieć dostęp do usług świadczonych w ramach rachunków płatniczych. Te usługi powinny być świadczone przez ASPSP na podstawie zasad obiektywnych, niedyskryminujących i proporcjonalnych. Każda odmowa świadczenia takich usług dla TPP powinna być należycie umotywowana i przedstawiona organowi nadzoru – Komisji Nadzoru Finansowego.

Dostawcy usług płatniczych będący TPP nie są zobligowani do nawiązywania jakiejkolwiek relacji umownej z ASPSP. Wymóg współpracy ASPSP z TPP wynika bezpośrednio z dyrektywy PSD II[77]. TPP w przypadku świadczenia usług inicjowania płatności nie wchodzi na żadnym etapie transakcji płatniczej w posiadanie środków pieniężnych. W przypadku, gdy TPP zamierza to robić, jest zobligowany do wystąpienia do Komisji Nadzoru Finansowego i uzyskania pełnego zezwolenia na świadczenie usług płatniczych.

---

[73] Por. K. Korus, *Pojęcie usługi płatniczej*…, s. 33.

[74] K. Korus trafnie wskazuje, że rachunki powiązane z kredytami mogą być rachunkami płatniczymi. Zob. K Korus, *Usługi oparte na dostępie*…, s. 86; także: *Rekomendacja Rady Prawa Bankowego i Zespołu ds. Regulacji Płatniczych Związku Banków Polskich w sprawie wybranych problemów interpretacyjnych ustawy o usługach płatniczych*, http://zbp.pl/public/repozytorium/dla_bankow/prawo/rada_prawa_bankowego/dzialalnosc/rekomendacja_grupa_robocza.doc [dostęp: 25 X 2017]; M. Mostowik, *Prawna ochrona informacji o rachunku*…, s. 33.

[75] K. Korus, *Usługi oparte na dostępie*…, s. 87.

[76] Tamże, s. 87–88.

[77] Por. motyw 30 do preambuły oraz art. 66 ust. 5 dyrektywy PSD II.

Usługa inicjowania płatności – uwagi ogólne

Usługa PIS ma w założeniu przyspieszać wykonanie umowy przez akceptanta (np. wysyłkę towaru przez sklep internetowy), daje mu bowiem gwarancję uzyskania zapłaty za towar lub usługi. Za pośrednictwem PIS zostaje zainicjowana określona płatność elektroniczna na rachunek płatniczy akceptanta, tak jakby użytkownik robił to osobiście. Zgoda na wykonanie transakcji płatniczej udzielona przez płatnika za pośrednictwem PIS jest równoznaczna ze zgodą na realizację takiej transakcji wyrażoną przez płatnika bezpośrednio dostawcy[78].

Modelowy schemat transakcji płatniczej przy udziale PIS polega na tym, że zlecenie płatnicze płatnika (np. osoby dokonującej zakupu towaru w środowisku internetowym) jest przekazywane przy udziale dostawcy usługi PIS do ASPSP za pośrednictwem bankowości elektronicznej, udostępnianej użytkownikowi przez ASPSP. Odbiorcą środków pieniężnych jest przeważnie sprzedawca towaru, którego łączy z dostawcą usługi PIS umowa o obsługę takich płatności[79]. Usługa PIS umożliwia dokonanie płatności w środowisku internetowym bez potrzeby posiadania innego instrumentu płatniczego, np. karty płatniczej[80].

Indywidualne dane uwierzytelniające służące do bezpiecznego uwierzytelniania użytkownika (potwierdzania jego tożsamości przez dostawcę), którymi posługuje się użytkownik lub dostawca usługi PIS, są wydawane przez dostawcę prowadzącego rachunek płatniczy[81].

Usługa PIS została unormowana w art. 4 pkt 15 i art. 66 dyrektywy PSD II. Polega ona na złożeniu przez dostawcę usługi PIS – na polecenie i w imieniu użytkownika – zlecenia płatniczego do ASPSP w celu przekazania środków pieniężnych na rachunek odbiorcy wskazany przez użytkownika[82]. Podstawową usługą płatniczą, która jest przedmiotem PIS, jest polecenie przelewu[83]. Głównymi dostawcami tego typu usług są takie marki, jak Sofort[84] oraz Trustly[85].

Usługa inicjowania płatności – zagadnienia regulacyjne

Dostawcą usługi PIS może być wyłącznie dostawca usług płatniczych mający taki status na podstawie przepisów ustawy o usługach płatniczych. W przypadku dostawcy mającego status instytucji płatniczej jest wymagane rozszerzenie posiadanego zezwolenia o świadczenie usług płatniczych w zakresie PIS i AIS[86]. Dostawca usługi PIS

[78] Art. 64 ust. 2 dyrektywy PSD II.

[79] K. Korus, *Usługi oparte na dostępie*…, s. 84.

[80] Motywy 28 i 29 do preambuły dyrektywy PSD II.

[81] Motywy 30 do preambuły dyrektywy PSD II.

[82] K. Korus, *Usługi oparte na dostępie*…, s. 84.

[83] W rozumieniu art. 3 ust. 4 UUP.

[84] https://www.sofort.com/pol-PL/kupujacy/sb/zakupy-online-z-sofort-banking/.

[85] https://trustly.com/pl/.

[86] Instytucje kredytowe w rozumieniu art. 4 ust. 1 pkt 1 *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów*

musi posiadać kapitał założycielski w wysokości 50 tys. euro[87], który powinien się składać co najmniej z jednego z następujących elementów:

- instrumentu kapitałowego,
- agio emisyjnego[88] związanego z instrumentami kapitałowymi,
- zysków zatrzymanych,
- skumulowanych innych całkowitych dochodów,
- kapitału rezerwowego[89].

Powyższe ma stanowić element gwarancyjny w przypadku wystąpienia niepożądanych zdarzeń związanych z działalnością TPP.

Dostawca usług płatniczych świadczący usługi PIS powinien mieć ubezpieczenie od odpowiedzialności cywilnej lub inną porównywalną gwarancję w celu możliwości pokrycia przez niego zobowiązań[90]. Ta regulacja i odpowiedni poziom zabezpieczenia mają szczególne znaczenie dla stabilności i bezpieczeństwa banku (lub innego podmiotu prowadzącego rachunek płatniczy), gdyż w przypadku wystąpienia nieautoryzowanej transakcji płatniczej inicjowanej przez dostawcę usługi PIS, to ASPSP (np. bank) zwraca bezzwłocznie, a w każdym wypadku nie później niż do końca następnego dnia roboczego, płatnikowi (klientowi) kwotę nieautoryzowanej transakcji[91]. W dalszej kolejności dostawca usługi PIS, w przypadku gdy jest odpowiedzialny za nieautoryzowaną transakcję, rekompensuje ASPSP straty poniesione lub sumy zapłacone w wyniku zwrotu na rzecz płatnika, łącznie z kwotą nieautoryzowanej transakcji płatniczej[92].

Artykuł 66 dyrektywy PSD II wprowadza do europejskiego porządku prawnego założenia i ramy regulujące usługę PIS. Fundamentalnymi sprawami są poniższe zagadnienia dotyczące wymogów regulacyjnych nałożonych na dostawcę usługi PIS oraz na ASPSP.

Obowiązki dostawcy usługi PIS[93]:

- dyrektywa PSD II przewiduje, że korzystanie z PIS jest prawem płatnika (użytkownika), a ASPSP musi respektować to uprawnienie;
- dostawca usługi PIS musi uzyskać zgodę płatnika na zainicjowanie zlecenia płatniczego;

---

ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz. Urz. UE L 176 z 27 czerwca 2013 r., s. 1) nie potrzebują takiego zezwolenia, zgodnie z art. 11 ust. 1 dyrektywy PSD II.

[87] Art. 7 pkt b) dyrektywy PSD II.

[88] Jest to różnica pomiędzy wartością nominalną określonego instrumentu kapitałowego, np. akcji, a jego ceną emisyjną.

[89] Art. 7 PSD II w zw. z art. 26 ust. 1 lit. a)-e) rozporządzenia PE i Rady (UE) nr 575/2013 w sprawie wymogów ostrożnościowych.

[90] Art. 5 ust. 2 dyrektywy PSD II.

[91] Art. 73 ust. 2 dyrektywy PSD II.

[92] Art. 73 ust. 2 zd. 2 dyrektywy PSD II.

[93] Art. 66 ust. 1 i 3 dyrektywy PSD II.

- prawo do korzystania z PIS przysługuje wyłącznie w przypadku, gdy ASPSP prowadzi dla użytkownika rachunek płatniczy dostępny online;
- dostawca usługi PIS przy świadczeniu usługi inicjowania płatności nie wchodzi w żadnym momencie w posiadanie środków pieniężnych płatnika;
- dostawca usługi PIS nie może zmieniać kwoty zlecenia płatniczego;
- dostawca usługi PIS nie może zmieniać odbiorcy zlecenia płatniczego;
- dostawca usługi PIS nie może zmieniać żadnych innych cech transakcji płatniczej;
- dostawca usługi PIS musi zagwarantować, aby indywidualne dane uwierzytelniające użytkownika nie były dostępne dla innych (niż użytkownik i wydawca tych danych) stron;
- dostawca usługi PIS musi zagwarantować, aby indywidualne dane uwierzytelniające użytkownika były przekazywane za pośrednictwem bezpiecznych i wydajnych kanałów;
- dostawca usługi PIS musi zagwarantować, aby wszelkie informacje o użytkowniku usług płatniczych były dostarczane wyłącznie odbiorcy i tylko za wyraźną zgodną użytkownika usług płatniczych;
- dostawca usługi PIS jest zobligowany – każdorazowo, gdy jest inicjowana płatność – do identyfikowania siebie wobec dostawcy usług płatniczych prowadzącego rachunek płatniczy płatnika (ASPSP);
- dostawca usługi PIS jest zobligowany – przy inicjowaniu płatności – do bezpiecznego porozumiewania się z ASPSP, płatnikiem i odbiorcą, zgodnie z postanowieniami art. 98 ust. 1 lit. d) dyrektywy PSD II[94];
- dostawca usługi PIS nie może przechowywać szczególnie chronionych danych dotyczących płatności;
- dostawca usługi PIS nie może żądać od użytkownika usług płatniczych innych danych niż dane niezbędne do wykonania usługi inicjacji płatności;
- dostawca usługi PIS nie może używać, uzyskiwać ani przechowywać żadnych danych do celów innych niż do wykonania usługi inicjowania płatności wyraźnie zleconej przez płatnika.

[94] Europejski Urząd Nadzoru Bankowego (EUNB) we współpracy z Europejskim Bankiem Centralnym (EBC) i po przeprowadzeniu konsultacji z wszystkimi stosownymi podmiotami zainteresowanymi, w tym podmiotami na rynku usług płatniczych, opracowuje projekt regulacyjnych standardów technicznych skierowanych do dostawców usług płatniczych, określających:

1) wymogi dotyczące silnego uwierzytelniania klienta,
2) wyłączenia ze stosowania silnego uwierzytelniania klienta,
3) wymogi, jakie muszą spełniać środki bezpieczeństwa, w celu ochrony poufności i integralności indywidualnych danych uwierzytelniających użytkowników usług płatniczych,
4) wymogi w zakresie wspólnych i bezpiecznych otwartych standardów komunikacji do celów identyfikowania, uwierzytelniania, powiadamiania i informowania, a także na potrzeby wdrożenia środków bezpieczeństwa, między dostawcami usług ASPSP, PIS, AIS, płatnikami, odbiorcami i innymi dostawcami usług płatniczych.

Obowiązki ASPSP[95]:

- ASPSP jest zobowiązany do porozumiewania się z dostawcą usługi PIS w sposób bezpieczny, zgodnie z postanowieniami art. 98 ust. 1 lit. d) dyrektywy PSD II;
- ASPSP bezzwłocznie po otrzymaniu zlecenia płatniczego od dostawcy usługi PIS jest zobowiązany do przekazania lub udostępniania mu wszystkich informacji o zainicjowaniu transakcji płatniczej oraz wszystkich informacji dostępnych dostawcy ASPSP w odniesieniu do wykonania transakcji płatniczej;
- ASPSP musi traktować zlecenia płatnicze przekazane za pośrednictwem dostawcy usługi PIS w sposób niedyskryminujący w stosunku do zleceń płatniczych przekazanych bezpośrednio ASPSP przez samego płatnika, szczególnie pod względem czasu wykonania, priorytetowego charakteru, opłat, co jednak nie dotyczy przypadku, gdy postępowanie dyskryminujące jest uzasadnione przyczynami obiektywnymi;
- świadczenie usług PIS nie może być uzależnione od istnienia stosunku umownego między dostawcą usługi PIS a ASPSP.

Usługa dostępu do informacji o rachunku – uwagi ogólne

Usługa AIS jest regulowana przez art. 4 pkt 16 oraz art. 67 dyrektywy PSD II. Polega ona na dostępie dostawcy tego typu usługi do rachunku płatniczego (bankowego) prowadzonego dla użytkownika. Dostawca usługi AIS dokonuje logowania do systemu bankowości elektronicznej użytkownika za jego zgodą, a następnie pobiera i przekazuje mu zagregowane informacje w komunikacji online. Uzyskuje w ten sposób dostęp do danych „na temat rachunku" oraz danych dotyczących wszystkich transakcji płatniczych na tym rachunku[96].

Usługa dostępu do informacji o rachunku – zagadnienia regulacyjne

Artykuł 67 dyrektywy PSD II wprowadza do europejskiego porządku prawnego ramy regulacyjne AIS. Świadczenie usług AIS nie wymaga uzyskania zezwolenia krajowego organu nadzoru (KNF), a wyłącznie rejestracji w tym organie[97]. Dostawca usługi AIS powinien posiadać ubezpieczenie od odpowiedzialności lub inną porównywalną gwarancję w celu możliwości pokrycia przez niego zobowiązań[98].

Obowiązki dostawcy usługi AIS:

- dyrektywa PSD II przewiduje, że korzystanie z AIS jest prawem płatnika (użytkownika), ASPSP zaś musi respektować to uprawnienie;

[95] Art. 66 ust. 4 dyrektywy PSD II.
[96] K. Korus, *Usługi oparte na dostępie*…, s. 85; także: art. 67 ust. 2 lit. d) dyrektywy PSD II.
[97] Art. 33 i 5 ust. 3 dyrektywy PSD II.
[98] Art. 5 ust. 3 dyrektywy PSD II.

- dostawca usługi AIS musi uzyskać zgodę użytkownika na świadczenie swoich usług dla niego;
- prawo do korzystania z usług AIS przysługuje użytkownikowi wyłącznie w przypadku, gdy ASPSP prowadzi dla użytkownika rachunek płatniczy dostępny online;
- dostawca usługi AIS musi zapewnić, aby indywidualne dane uwierzytelniające użytkownika nie były dostępne dla innych stron, z wyjątkiem użytkownika i wydawcy indywidualnych danych uwierzytelniających użytkownika;
- dostawca usługi AIS musi zapewnić, aby indywidualne dane uwierzytelniające użytkownika były przekazywane przez dostawcę świadczącego usługi AIS za pośrednictwem bezpiecznych i wydajnych kanałów;
- dostawca usługi AIS musi w przypadku każdej sesji komunikacyjnej identyfikować siebie wobec ASPSP;
- dostawca usługi AIS musi porozumiewać się z ASPSP i użytkownikiem w sposób bezpieczny – zgodnie z art. 98 ust. 1 lit. d) dyrektywy PSD II;
- dostawca usługi AIS może uzyskiwać dostęp wyłącznie do informacji dotyczących wyznaczonych rachunków płatniczych i związanych z nimi transakcji płatniczych;
- dostawca usługi AIS nie może żądać szczególnie chronionych danych dotyczących płatności związanych z rachunkami płatniczymi;
- dostawca usługi AIS nie może używać, uzyskiwać ani przechowywać żadnych danych do celów innych niż do wykonania usługi dostępu do informacji o rachunku, wyraźnie zleconej przez użytkownika usług płatniczych zgodnie z przepisami o ochronie danych.

Obowiązki ASPSP:

- ASPSP musi porozumiewać się z dostawcą usługi AIS w sposób bezpieczny i zgodny z postanowieniami art. 98 ust. 1 lit. d) dyrektywy PSD II;
- ASPSP musi traktować wnioski o udostępnienie danych przekazane za pośrednictwem dostawcy usługi AIS w sposób niedyskryminujący, chyba że postępowanie dyskryminujące jest uzasadnione przyczynami obiektywnymi;
- świadczenie usług AIS nie może być uzależnione od istnienia stosunku umownego między dostawcą usługi AIS a ASPSP;
- zgodnie z motywem 28 do preambuły dyrektywy PSD II ASPSP udostępnia wszystkie informacje dotyczące rachunku płatniczego, przede wszystkim: numer IBAN lub NRB, wysokość salda, historię transakcji (kwotę, tytuł, datę wykonania, dane drugiej strony[99]).

[99] M. Mostowik, *Prawna ochrona informacji o rachunku*…, s. 34.

Głównymi dostawcami tych usług są takie podmioty, jak: Kontomierz[100], AFAS[101], tink[102], Money Dashboard[103] i Quontis[104].

Potwierdzenie dostępności środków pieniężnych na rachunku płatniczym – uwagi ogólne

Dyrektywa PSD II wprowadza oprócz powyższych usług TPP także proces potwierdzania dostępności środków pieniężnych na rachunku płatniczym płatnika. Ten proces nie jest jednak ujęty w regulacjach jako odrębna usługa płatnicza. Umożliwia wydawcy instrumentu płatniczego opartego na karcie płatniczej[105] – uprzednio wskazanemu ASPSP przez użytkownika, którego rachunek płatniczy ASPSP dostarcza – domaganie się od ASPSP w czasie rzeczywistym, przy użyciu komunikacji online, informacji, czy na rachunku użytkownika znajduje się określona kwota. Proces potwierdzania dostępności środków pieniężnych reguluje zatem obowiązki ASPSP wobec wydawcy instrumentu płatniczego opartego na karcie płatniczej. Obowiązkiem użytkownika jest wcześniejsze poinformowanie ASPSP o zamiarze korzystania z CAF[106].

Potwierdzenie dostępności środków pieniężnych na rachunku płatniczym – zagadnienia regulacyjne

Obowiązkiem ASPSP jest potwierdzenie – na wniosek dostawcy wydającego instrumenty płatnicze oparte na karcie – dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej realizowanej na podstawie karty[107] (usługa CAF).

Wymogi prawne do stosowalności usługi CAF[108]:

- rachunek płatniczy płatnika musi być dostępny za pośrednictwem Internetu w momencie występowania z wnioskiem o potwierdzenie dostępności środków pieniężnych;
- płatnik musi udzielić ASPSP zgody na odpowiadanie na wnioski określonego dostawcy usług płatniczych w celu potwierdzenia, że kwota odpowiadająca

[100] http://kontomierz.pl.
[101] https://www.afas.nl.
[102] https://www.tinkapp.com/en/.
[103] https://www.moneydashboard.com.
[104] http://www.qontis.ch.
[105] Instrument oparty na karcie płatniczej to dowolny instrument płatniczy (m.in. karta, telefon komórkowy, komputer) umożliwiający zainicjowanie transakcji płatniczej z wykorzystaniem infrastruktury systemu kart płatniczych, por. art. 2 pkt 20 rozporządzenia PE i Rady (UE) 2015/751 w sprawie opłat interchange w odniesieniu do transakcji płatniczych.
[106] K. Korus, *Usługi oparte na dostępie*…, s. 85.
[107] Art. 65 ust. 1 dyrektywy PSD II.
[108] Tamże.

określonej transakcji płatniczej realizowanej na podstawie karty jest dostępna na rachunku płatniczym płatnika;
– zgoda dla ASPSP od użytkownika dotyczącą odpowiadania na wnioski musi być udzielona przed wystąpieniem z pierwszym wnioskiem o potwierdzenie.

Wymogi prawne nałożone na dostawcę występującego z wnioskiem:

– płatnik musi udzielić dostawcy wyraźnej zgody na występowanie z wnioskiem o potwierdzenie dostępności środków pieniężnych;
– płatnik musi zainicjować transakcję płatniczą realizowaną przy użyciu instrumentu płatniczego opartego na karcie;
– dostawca usługi CAF musi uwierzytelnić samego siebie wobec dostawcy ASPSP;
– dostawca usługi CAF musi porozumiewać się z ASPSP w sposób bezpieczny, zgodnie z postanowieniami art. 98 ust. 1 lit. d) dyrektywy PSD II.

Potwierdzenie dostępności środków pieniężnych na rachunku płatniczym przez ASPSP ma polegać na udzieleniu odpowiedzi „tak" lub „nie". Stan salda nie jest podawany. Dostawca usługi CAF nie może przechowywać ani wykorzystywać odpowiedzi uzyskanej od ASPSP do celów innych niż wykonanie transakcji płatniczej realizowanej na podstawie karty[109]. Potwierdzenie dostępności środków nie daje możliwości blokowania przez ASPSP określonej kwoty na rachunku płatnika do czasu rozliczenia płatności[110].

W celu wykonywania usługi CAF niezbędne jest zezwolenie na wydawanie instrumentów płatniczych opartych na karcie.

Działalność TPP a cyberbezpieczeństwo

Zapobieganiem i przeciwdziałaniem cyberprzestępczości w zakresie infrastruktury płatniczej powinny zająć się oprócz uprawnionych podmiotów publicznych także branżowe organizacje finansowe[111] (we współpracy z właściwymi służbami publicznymi) jako podmioty bezpośrednio narażone na zagrożenie cyberprzestępczością i zainteresowane poprawą cyberbezpieczeństwa. Przykładem takiej organizacji jest FinansCERT z Norwegii[112]. Ta organizacja jest CERT-em[113] w norweskim sektorze finansowym: bankowym i ubezpieczeniowym. Do jej głównych zadań należą:

– śledzenie zagrożeń zewnętrznych,
– wsparcie w zwalczaniu ataków i ograniczaniu strat,
– koordynacja współpracy z instytucjami publicznymi i służbami porządkowymi (Interpol, Policja).

[109] Art. 65 ust. 3 dyrektywy PSD II.
[110] Art. 65 ust. 4 dyrektywy PSD II.
[111] Zob. A. Marciniak, *Bankowy CERT – nowa broń*…
[112] FinansCERT jako organizacja została powołana 23 IV 2013 r. przy norweskiej branżowej organizacji zrzeszającej instytucje finansowe, http://www.finanscert.no [dostęp: 15 X 2017].
[113] Computer Emergency Response Team (z ang. zespół reagowania na incydenty komputerowe).

Innymi organizacjami branżowymi, których przedmiotem działalności jest zwalczanie zagrożeń w zakresie bezpieczeństwa informacji, są m.in.: National Cyber-Forensics & Training Alliance (NCFTA), Financial Services Information Sharing and Analysis Center (FS-ISAC), Soltra czy działająca w Unii Europejskiej European Financial Institutes – Information Sharing and Analysis Centre (FI-ISAC)[114] tj. organizacje pozarządowe o globalnym zasięgu mające siedziby w Stanach Zjednoczonych.

Bankowe Centrum Cyberbezpieczeństwa

We wrześniu 2015 r. z inicjatywy Rady Bankowości Elektronicznej działającej przy Związku Banków Polskich (ZBP) została wydana rekomendacja dotycząca bezpieczeństwa oraz zapobiegania brakowi dostępu do bankowości elektronicznej. Rekomendacja zawiera zalecenie, aby banki zrzeszone w ZBP nawiązały współpracę w zakresie:

- przeciwdziałania atakom na platformy bankowości elektronicznej banków oraz ich klientów,
- reagowania na ataki.

Rezultatem tej rekomendacji było powołanie Bankowego Centrum Cyberbezpieczeństwa (BCC)[115]. BCC stanowi obecnie jedną z najważniejszych platform Narodowego Centrum Cyberbezpieczeństwa (NC Cyber)[116]. Współpracuje z Policją oraz Krajową Izbą Rozliczeniową SA, operatorami telekomunikacyjnymi, operatorami szybkich płatności i giełdami bitcoin[117]. W przypadku zagrożenia cyberbezpieczeństwa BCC staje się sztabem kryzysowym zarządzającym sytuacją kryzysową w sektorze bankowym. Aktualnie obszarami zainteresowania BCC są przede wszystkim:

- monitoring sektora bankowego w zakresie cyberbezpieczeństwa i reagowania na zagrożenia;
- zarządzanie komunikacją zwłaszcza przez:
  - opracowanie spójnej polityki informacyjnej w stosunku do klientów i mediów w sektorze bankowym, której głównym założeniem jest niezwłoczne informowanie o wszelkich zagrożeniach cyberbezpieczeństwa lub awariach systemów bankowości elektronicznej,

[114] A. Marciniak, *Bankowy CERT – nowa broń*…

[115] Por. informację o otwarciu BCC udostępnioną na stronie internetowej ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/lipiec/otwarcie-bankowego-centrum-cyberbezpieczenstwa [dostęp: 25 X 2017]; zob. odpowiedź A. Stróżyńskiej na interpelację, BM-WOP.072.69.2017, Warszawa 22 VI 2017 r., http://www.sejm.gov.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=75AD31FB, [dostęp: 25 X 2017]; A. Marciniak, *Bankowy CERT – nowa broń*…

[116] NCC zostało powołane 4 VII 2016 r. i działa w strukturze NASK (Naukowej i Akademickiej Sieci Komputerowej), która jest państwowym instytutem badawczym w rozumieniu *Ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych* (t.j.: Dz.U. z 2018 r. poz. 736) oraz par. 3 ust. 2 pkt 1 ppkt d) *Rozporządzenia Rady Ministrów z dnia 7 czerwca 2017 w sprawie nadania Naukowej i Akademickiej Sieci Komputerowej statusu państwowego instytut badawczego* (Dz.U. z 2017 r. poz. 1193). Do zadań NASK należy zapewnianie cyberbezpieczeństwa podmiotom publicznym przez rozwój Narodowego Centrum Cyberbezpieczeństwa.

[117] A. Marciniak, *Bankowy CERT – nowa broń*...

- opracowanie procedur komunikacji pomiędzy uczestnikami,
- opracowanie procedur współpracy i kanałów komunikacji z organami ścigania, innymi CERT-ami, producentami oprogramowania oraz opracowanie systemów zabezpieczeń;

– definiowanie i monitorowanie wdrażania działań prewencyjnych w sektorze[118].

Z łatwością można sobie wyobrazić sytuację, w której TPP w początkowej fazie działalności – budując swoją reputację na rynku oraz zaufanie użytkowników i po jakimś czasie dysponując już danymi, które umożliwiają zalogowania się do rachunków bankowych klientów – doprowadza na masową skalę do wielu nieautoryzowanych transakcji. Za te transakcje wobec klientów rzekomo korzystających z usługi PIS w pierwszej kolejności prawnie i finansowo odpowiada bank. Bank występuje do TPP z roszczeniem o zwrot należności będących przedmiotem nieautoryzowanych transakcji. To roszczenie może być zaspokojone tylko pod warunkiem, że TPP jest wypłacalny. Można podać także inny przykład, gdy dostawca usługi AIS posiadający bazę danych wrażliwych uprawniających do zalogowania się do kont bankowych, doprowadza umyślnie do utraty takiej bazy. Koszty, nie tylko finansowe (powodowane dużą liczbę transakcji płatniczych o ogromnej wartości), lecz także społeczne (powodowane utratą zaufania klientów do systemu płatniczego) mogą być trudne do oszacowania. Nawet w przypadku gdy wyrządzona szkoda zostanie pokryta w pełni, istotnym kosztem będzie utrata zaufania do sektora finansowego przez klientów.

Biorąc powyższe pod uwagę, należy stwierdzić, że działalność TPP może powodować także problemy prawne na płaszczyźnie:

– tajemnicy bankowej[119],
– tajemnicy płatniczej[120],
– prawa do ochrony danych osobowych,
– prawa do prywatności, zarówno dla posiadacza rachunku, jak i osób trzecich, których dane osobowe widnieją w aplikacji bankowości elektronicznej jako płatnicy lub odbiorcy[121].

Podsumowanie

Usługi TPP są i nadal będą wykonywane w segmencie płatności elektronicznych, a ich jeszcze większy wzrost nastąpi wtedy, gdy zostaną na stałe połączone z dostawcami portali społecznościowych i usług masowych, takich tak: Facebook, Apple, Amazon, Netflix, Google[122], Uber, Spotify.

[118] Tamże, s. 193.

[119] Zob. art. 104 ust. 1 *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* (t.j.: Dz.U. z 2017 r. poz. 1876, ze zm.).

[120] Zob. art. 11 ust. 1 UUP.

[121] W zakresie wskazanych rodzajów ryzyka por. M. Mostowik, *Prawna ochrona informacji o rachunku…*, s. 35–42.

[122] Określanych w skrócie FAANG (Facebook, Apple, Amazon, Netflix, Google).

Zarówno dostawcy świadczący usługi inicjowania płatności (PIS) oraz usługę dostępu do rachunku płatniczego (AIS) po jednej stronie, jak i dostawcy tradycyjnych usług płatniczych po drugiej powinni przestrzegać wymogów dotyczących ochrony danych i bezpieczeństwa wynikających z dyrektywy PSD II oraz RTS. Regulacyjne standardy techniczne powinny zapewnić interoperacyjność[123] różnych rozwiązań komunikacyjnych z technologicznego punktu widzenia. Ponadto dzięki regulacyjnym standardom technicznym dostawca prowadzący rachunek płatniczy (ASPSP) ma możliwość zorientowania się, czy przy przeprowadzaniu danej transakcji płatniczej kontaktuje się z nim dostawca PIS, a nie bezpośrednio jego klient[124].

Należy zwrócić uwagę, że regulacje w dyrektywie PSD II w zakresie działalności TPP są bardzo ogólne. Wszystkie istotne sprawy techniczne, które mają zapewnić bezpieczeństwo tych usług oraz podmiotów z nich korzystających i je dostarczających, zostały rozstrzygnięte przez RTS. Z uwagi na to, że usługi TPP są świadczone między innymi w środowisku internetowym, nieprawidłowości w ich funkcjonowaniu mogą zagrażać cyberbezpieczeństwu płatniczej infrastruktury krytycznej. Związek Banków Polskich stale monitoruje sytuację rzeczywistą i prawną. Zwraca przy tym uwagę na zagrożenia związane z działalnością TPP[125].

Zapisy prawne zawarte w dyrektywnie PSD II dotyczące TPP są przykładem skutecznego lobbingu regulacyjnego podmiotów świadczących od lat usługi omawiane w artykule. Podmioty będące TPP z uwagi na potencjalne zagrożenia w skali mikro (utrata środków finansowych przez użytkownika) i makro (zagrożenie funkcjonowania płatniczej infrastruktury krytycznej) powinny spotkać się z ostrożnym podejściem do tych podmiotów ze strony regulatora – Komisji Nadzoru Finansowego oraz użytkowników w początkowej fazie ich funkcjonowania.

Bibliografia:

Chinowski B., *Elektroniczne metody płatności. Istota, rozwój, prognozy*, https://www.knf.gov.pl/knf/pl/komponenty/img/Elektroniczne%20metody%20platnosci.pdf [dostęp: 20 X 2017].

Grabowski M., *Instrumenty płatnicze w prawie polskim*, Warszawa 2013, CeDeWu.

Grabowski M., *Ustawa o usługach płatniczych. Komentarz*, Warszawa 2012, C.H. Beck.

Gradzi D., *Bezpieczeństwo płatności elektronicznych jako element cyberbezpieczeństwa państwa – przegląd regulacji prawnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 38–54.

[123] Cecha produktu lub systemu, którego interfejsy umożliwiają współpracę z innymi produktami lub systemami.

[124] Motyw 93 do preambuły dyrektywy PSD II.

[125] Por. *Notatkę dotyczącą usług opartych o dostęp stron trzecich (PISP, AISP) do rachunków płatniczych w świetle PSD2 Rady Bankowości Elektronicznej Związku Banków Polskich*, https://zbp.pl/public/repozytorium/wydarzenia/images/luty_2017/Polish_Bank_Association_Notatka_PL_Third_Party_Services_PSD2_January_2017_fin.pdf [dostęp: 10 X 2017].

Kaszubski R., Obzejta Ł., *Karty płatnicze w Polsce*, Warszawa 2012, Wolters Kluwer.

Korus K., *Pojęcie usługi płatniczej w ustawie o usługach płatniczych*, „Monitor Prawa Bankowego" 2012, nr 7–8, s. 43–58.

Korus K., *Usługi oparte na dostępie do rachunku w dyrektywie PSD II*, „Monitor Prawa Bankowego" 2017, nr 7–8, s. 81–93.

Maison D., *Postawy Polaków wobec obrotu bezgotówkowego. Raport z badania 2016 i analiza porównawcza z danymi z 2009 i 2013 r.*, https://www.nbp.pl/badania/seminaria/8v2017.pdf [dostęp: 10 X 2017].

Marciniak A., *Bankowy CERT – nowa broń w walce z cyberprzestępczością*, w: *Wyzwania informatyki bankowej 2016,* A. Kawiński, A. Sieradz (red.), Gdańsk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf [dostęp: 2 X 2017].

Mostowik M., *Prawna ochrona informacji o rachunku płatniczym w świetle usługi dostępu do informacji o rachunku (AIS)*, „Monitor Prawa Bankowego" 2017, nr 7–8, s. 35–42.

Pacak M., *Usługi płatnicze. Komentarz*, Warszawa 2014, LexisNexis.

Radziejewski K., *Cyberbezpieczeństwo w administracji rządowej w Rzeczpospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 308–330.

Staszczyk M., *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, http://www.finanseiprawofinansowe.uni.lodz.pl/Publikacje/5/4_Staszczyk.pdf [dostęp: 2 X 2017].

Akty prawne:

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) 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L 337 z 23 grudnia 2015 r., s. 35).

Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48 WE i uchylająca dyrektywę 97/5/WE (Dz. Urz. UE L 319 z 5 grudnia 2007, s. 1).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j.: Dz.U. z 2017 r. poz. 2003, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j.: Dz.U. z 2018 r. poz. 1401).

Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (t.j.: Dz.U. z 2018 r. poz. 145, ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j.: Dz.U. z 2017 r. poz. 1876, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: Dz.U. z 2017 r. poz. 2204, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j.: Dz.U. z 2018 r. poz. 452, ze zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz. Urz. UE L 176 z 27 kwietnia 2013 r., s. 1).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę (Dz. Urz. UE L 123 z 19 maja 2015, s. 1).

Projekt ustawy o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw, numer z wykazu: UC81.

Abstrakt

Płatności internetowe i mobilne z uwagi na ich bezgotówkowy charakter i szybkość dokonywania transakcji cechują się dużym potencjałem rozwojowym. Wraz ze wzrostem ich wolumenu ilościowego i kwotowego rosną także zagrożenia związane z ich procesowaniem, ponieważ odbywają się one bez fizycznego udziału stron transakcji i w środowisku internetowym. Nowe metody płatności doprowadziły do pojawienia się nowych dostawców usług płatniczych – tzw. *Third Party Payment Service Providers*, tj. dostawców będących podmiotami trzecimi, których działalność może się wiązać z określonymi zagrożeniami. W skali mikro można stypizować zagrożenia związane z bezpieczeństwem środków finansowych użytkowników. W skali makro należy wskazać na potencjalne zagrożenia tzw. płatniczej infrastruktury krytycznej i szerzej – cyberbezpieczeństwa.

Słowa kluczowe: dyrektywa PSD, cyberprzestępczość, *Third Party Providers*, infrastruktura krytyczna, Komisja Nadzoru Finansowego, elektroniczne transakcje płatnicze, płatności mobilne, płatności internetowe, *Account Servicing Payment Service Provider*, *Account Information Service*, *Payment Initiation Service*.