TOM LXXII • NR 12 (858) • DOI 10.33226/0137-5490.2019.12.3

Silne uwierzytelnianie klienta w świetle przepisów normujących wymogi bezpieczeństwa płatności — wybrane problemy

Strong customer authentication in the light of regulations — selected problems

dr hab. Anna Zalcewicz

Profesor w Zakładzie Prawa Gospodarczego i Polityki Gospodarczej
na Wydziale Administracji i Nauk Społecznych Politechniki Warszawskiej
E-mail: a.zalcewicz@ans.pw.edu.pl; nr ORCID: 0000-0002-2459-4398

Streszczenie

Celem niniejszego artykułu jest dokonanie analizy przepisów prawa normujących środki bezpieczeństwa przy stosowaniu silnego uwierzytelniania klienta (*strong customer authentication*, SCA). Wprowadzone przez dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE (Dz.Urz. UE L 337, s. 35) zasady dotyczące identyfikacji tożsamości przy dokonywaniu płatności poprzez stosowanie SCA mają ograniczyć ryzyko nadużyć i oszustw, zwiększyć bezpieczeństwo płatności poprzez wprowadzenie rozwiązań zmniejszających możliwość dokonania nieautoryzowanych lub nielegalnych transakcji płatniczych. Znaczący wpływ tych przepisów na konsumentów przy jednoczesnej złożoności wymogów sprawia, że szczególnie istotne jest podjęcie rozważań ukierunkowanych na dokonanie takich analiz i podjęcie próby identyfikacji potencjalnych zagrożeń w związku z ingerencją prawodawczą w ten obszar usług płatniczych.
W niniejszym artykule zwraca się również uwagę na zjawisko technologizacji prawa rynku usług płatniczych, a szerzej - rynku finansowego.

Słowa kluczowe: prawo, usługi płatnicze

Summary

The purpose of this article is to analyze the law that regulates security measures when applying strong customer authentication (SCA). The rules introduced by PSD2 regarding identity identification when making payments through the use of SCA are to reduce the risk of fraud and increase payment security by introducing solutions that reduce the possibility of making unauthorised or fraudulent payment transactions. The significant impact of these provisions on consumers with the simultaneous complexity of the requirements makes it particularly important to undertake considerations aimed at conducting such analyzes and attempting to identify potential threats in connection with legislative interference in this area of payment services.
This article also draws attention to the phenomenon of technologization of the payment services market law, and more broadly the financial market.

Key words: law, payment services

Wprowadzenie

Nowe możliwości technologiczne sprawiają, że znacząco wzrasta liczba płatności dokonywanych bezgotówkowo z wykorzystaniem niestosowanych wcześniej rozwiązań technicznych. Zwiększającej się innowacyjności płatności elektronicznych towarzyszą nowe wyzwania normatywne w obszarze regulacji rynku usług płatniczych związane m.in. z zapewnieniem bezpieczeństwa płatności elektronicznych i ochrony konsumenta. Można postawić tezę, że obecnie następuje coraz wyraźniejsza technologizacja prawa rynku finansowego, rozumiana jako przenoszenie na poziom regulacyjny wymogów technicznych służących zapewnieniu innowacyjności i bezpieczeństwa usług, a także szeroko pojętej ochronie

klienta obejmującej zarówno kwestie percepcji komunikatów adresowanych do klientów i potencjalnych klientów, wykluczenia na skutek zastosowań nowych technologii, jak i standardów świadczenia usług. W ramach tego nowego zjawiska obecnie obserwować można sformalizowanie zasad dotyczących bezpieczeństwa płatności, którego elementem jest silne uwierzytelnienie klienta i spójność podejścia do tej kwestii we wszystkich państwach Europejskiego Obszaru Gospodarczego (EOG), a dostawcy usług płatniczych zostali zobligowani do stosowania tego rodzaju uwierzytelniania w przypadkach określonych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE (Dz.Urz. UE L 337, s. 35), dalej PSD2. Wpisuje się to w ogólnie przyjęty w PSD2 model szerszej ochrony klienta i zwiększenia praw konsumenta w wielu obszarach, jak np. zmniejszenie odpowiedzialności konsumentów za nieautoryzowane płatności, ochrona danych konsumentów itd. (na ten temat szerzej Byrski, 2017, s. 25–42).

W związku ze zmianami prawodawczymi w zakresie uwierzytelniania właściwe wydaje się podjęcie rozważań, jaki jest obecnie zakres tych regulacji. Celem niniejszego artykułu jest w związku z tym dokonanie analizy przepisów prawa normujących silne uwierzytelnienie klienta przede wszystkim z punktu widzenia określonych w przepisach kategorii (wiedza, posiadanie, cechy klienta), a także identyfikacja potencjalnych zagrożeń w związku z ingerencją prawodawczą w ten obszar usług płatniczych.

Źródła prawa

Dążenie do stworzenia jednolitego obszaru płatności oraz określenia zasad funkcjonowania efektywnego rynku usług płatniczych w państwach EOG skutkuje ingerencją prawodawcy unijnego w ten segment rynku. Nie bez znaczenia dla regulacji rynku usług płatniczych pozostaje również *soft law* (zob. szerzej Fedorowicz, Zalcewicz, 2019). Przyjęcie dyrektywy 2007/64/WE Parlamentu Europejskiego i Rady z 13.11.2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylającej dyrektywę 97/5/WE, Dz.Urz. UE L 319, s. 1, ze zm.), dalej PSD1, umożliwiło m.in. określenie wymogów dotyczących świadczenia usług płatniczych, a także praw i obowiązków użytkowników usług płatniczych, wprowadzenie wspólnych zasad dotyczących płatności elektronicznych i bezgotówkowych (polecenia przelewu, polecenia zapłaty, płatności kartą, płatności mobilne i internetowe), a także dalszy intensywny rozwój tej części rynku finansowego. Część rozwiązań przyjętych w 2009 r.[1] przestało jednak przystawać do nowych warunków gospodarczych i technicznych, pojawiły się też nowe wyzwania związane z funkcjonowaniem rynku usług płatniczych, co spowodowało, że konieczne stało się wprowadzenie nowych rozwiązań prawnych.

Z drugiej strony, w zakresie analizowanych zagadnień należy zaznaczyć, że w PSD1 kwestie wymogów bezpieczeństwa płatności nie były normowane, a rozwiązania dotyczące bezpiecznego uwierzytelniania były przedmiotem wytycznych lub rekomendacji (zob. np. European Central Bank, 2013; European Banking Authority, 2014). Stan ten zmienił się wraz z przyjęciem i transponowaniem PSD2. Wśród celów, jakie postawił sobie prawodawca unijny, co jest istotne w kontekście prowadzonych rozważań, jest „rozwój zintegrowanego rynku wewnętrznego bezpiecznych płatności elektronicznych" (motyw 5 preambuły PSD2) oraz zapewnienie wysokiego poziomu „ochrony konsumentów przy korzystaniu z tych usług płatniczych w całej Unii" (motyw 6 preambuły PSD2). Bezpieczeństwo to utożsamiane jest w dużym stopniu z dążeniem do eliminacji czy też ograniczenia zagrożeń, jakie niesie ze sobą użycie technologii przy korzystaniu z usług płatniczych oferowanych drogą elektroniczną, w tym ryzyka oszustw, a PSD2 za odpowiedni instrument w tym zakresie uznaje bezpieczne uwierzytelnianie użytkownika (motyw 95 preambuły PSD2). Dyrektywa ta staje się w związku z tym pierwotnym źródłem regulacji w tym zakresie. Jednocześnie zawiera normy kompetencyjne do opracowania regulacyjnych standardów technicznych dla EUNB oraz przyjęcia ich przez Komisję zgodnie z przepisami rozporządzenia (UE) nr 1093/2010 z 24.11.2010 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, s. 12 ze zm.) — art. 98 PSD2[2]. Pomimo że normy określające podstawowe wymagania w zakresie bezpieczeństwa płatności zawarto w PSD2 i RTS, to jednak sformalizowanie wymagań bezpieczeństwa płatności ma miejsce w prawie krajowym (European Banking Authority, 2019). W Polsce w związku z wejściem w życie ustawy z 10.05.2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (Dz.U. poz. 1075), dodano do ustawy z 19.08.2011 r. o usługach płatniczych (Dz.U. z 2019 r. poz. 659 ze zm.), dalej u.u.p., art. 32i normujący silne uwierzytelnianie klienta oraz wzbogacono słowniczek pojęciowy o pkt 26aa, w którym ujęto definicję silnego uwierzytelniania.

Termin wejścia w życie rozwiązań w zakresie PSD2 określono na 14.09.2019 r. we wszystkich państwach EOG, jednak możliwe było przyznanie dodatkowego czasu przez krajowe organy nadzoru na dostosowanie się do wymogów PSD2 w tym zakresie (co miało miejsce np. w przypadku Wielkiej Brytanii[3]). Niemniej jednak dostawcy usług płatniczych, nawet w przypadku ustalenia takiego terminu po 13.09.2019 r., ponoszą ryzyko wynikające z niestosowaniem SCA[4].

Silne uwierzytelnianie klienta jako pojęcie normatywne

Definicja legalna określenia „silne uwierzytelnianie klienta" zawarta jest w PSD2 oraz ustawie o usługach płatniczych. Obie definicje są zbieżne i opierają się na tych samych elementach. Po pierwsze, silne uwierzytelnianie musi odwoływać się do określonych w przepisach kategorii (wiedza, posia-

danie, cechy klienta); po drugie, kategorie te muszą być niepowiązane ze sobą w tym znaczeniu, że nie wpływają wzajemnie na wiarygodność dokonywanej weryfikacji użytkownika; po trzecie, uwierzytelnianie musi zapewnić ochronę poufności danych.

Dokonując szczegółowej analizy znaczenia zwrotu „silne uwierzytelnianie klienta" oraz pewnej jego kategoryzacji, można w pierwszej kolejności zaakcentować fakt, że samo uwierzytelnienie oznacza określoną procedurę. Jest to procedura, która umożliwia dostawcy usług płatniczych weryfikację tożsamości użytkownika usług płatniczych lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika (art. 4 pkt 29 PSD2 oraz art. 2 pkt 33b u.u.p.)[5]. Jak wskazano w RTS, procedura ta ma z jednej strony pozwalać na wychwytywanie prób nieuprawnionego użycia danych uwierzytelniających (m.in. danych skradzionych, przywłaszczonych), to jest nieautoryzowanych lub nielegalnych transakcji płatniczych, z drugiej, zapewniać, że z usługi płatniczej oferowanej drogą elektroniczną korzysta uprawniony użytkownik usług płatniczych (motyw 1 preambuły RTS oraz art. 2 ust. 1 RTS). W związku z tym, że procedura ta może przebiegać w różny sposób, zapewniając większy albo mniejszy poziom bezpieczeństwa transakcji, prawodawca unijny dokonał rozróżnienia na szczególny typ uwierzytelnienia, mający zmniejszyć ryzyko dokonania oszustwa przy przeprowadzaniu płatności elektronicznych, określając go mianem silnego uwierzytelnienia klienta (*strong customer authentication*, SCA).

Należy również wskazać, że przywołane definicje z ustawy o usługach płatniczych oraz PSD2 zostały uzupełnione przez RTS. Zgodnie z art. 2 RTS w SCA uwierzytelnianie ma nie tylko opierać się na co najmniej dwóch elementach, ale także prowadzić do wygenerowania kodu uwierzytelniającego. Ponadto należy wskazać, że w PSD2 wprowadzone są również dodatkowe wymogi w zakresie SCA, w przypadku gdy płatnik inicjuje elektroniczną transakcję płatniczą. Zgodnie bowiem z art. 97 ust. 2 PSD2 w przypadku elektronicznych zdalnych transakcji płatniczych dostawcy usług płatniczych są zobligowani do stosowania SCA obejmującego elementy, które dynamicznie łączą transakcję z określoną kwotą i określonym odbiorcą.

Reasumując, silne uwierzytelnienie klienta jest procesem, w którym dla zmniejszenia ryzyka nadużyć, w szczególności zmniejszenia możliwości dokonania oszustw płatniczych, stosowane są szczególne środki bezpieczeństwa, wśród których normuje się wymogi dotyczące: kategorii „wiedza", „posiadanie", „cechy klienta", niezależności elementów, kodu uwierzytelniającego oraz dynamicznego połączenia. Prawodawca unijny precyzuje również, kiedy SCA jest obowiązkowe dla dostawców usług płatniczych (art. 97 ust. 1 PSD2).

Wymogi odnośnie do elementów będących integralną częścią silnego uwierzytelniania klienta

Jak już wskazano, silne uwierzytelnienie dokonywane jest w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii „wiedza", „posiadanie" albo „cechy klienta". Elementy te zostały bliżej doprecyzowane w RTS.

Począwszy od pierwszej grupy, wyróżnionej jako „coś, co wie wyłącznie użytkownik" (wiedza), dotyczy ona zasobu informacji posiadanych przez korzystającego z usługi płatniczej wykorzystywanych przy dokonywaniu płatności do potwierdzenia deklarowanej tożsamości. Poszukując odpowiedzi na pytania, co technicznie spełnia w tym zakresie kryteria PSD2, doprecyzować można, że element wiedzy powinien istnieć przed rozpoczęciem płatności lub dostępu online (European Banking Authority, 2018), a także że istotna jest długość i złożoność elementu opierającego się na wiedzy (motyw 6 preambuły RTS). W szczególności do kategorii tej zaliczyć można, zgodnie z obowiązującymi przepisami, określone hasło, pin czy oparte na wiedzy odpowiedzi na pytania. Nie można tu kwalifikować natomiast numeru CVV czy daty ważności wydrukowanych na karcie ani adresu e-mail — ze względu na niespełnienie warunku wyłączności wiedzy użytkownika (European Banking Authority, 2018, pkt 32–34, zob. też Regnard-Weinrabe, Finlayson-Brown, 2019, s. 35 i n.).

Drugim elementem jest „posiadanie", czyli zgodnie z art. 4 pkt 30 PSD2 „coś, co posiada tylko użytkownik". Wymogi dotyczące tego elementu określa art. 7 RTS oraz przepisy normujące zasady zapewnienia poufności i integralności indywidualnych danych uwierzytelniających użytkowników usług płatniczych (art. 22–27 RTS).

W przypadku regulacji silnego uwierzytelniania termin „posiadanie" ma inne znaczenie niż to przyjęte na gruncie prawa cywilnego. W świetle przepisów PSD2 i RTS posiadanie nie oznacza ograniczonego prawa rzeczowego w rozumieniu ustawy z 23.04.1964 r. — Kodeks cywilny (Dz.U. z 2019 r. poz. 1145 ze zm.). W szczególności nie odnosi się wyłącznie do rzeczy, ale również do przedmiotów niematerialnych, np. aplikacji (pod warunkiem zapewnienia unikalnego połączenia z urządzeniem) (European Banking Authority, 2019). Wśród przykładów wymogów dotyczących elementów zaliczanych do kategorii „posiadanie" motyw preambuły 6 RTS wskazuje długość algorytmów, długość klucza oraz entropię informacyjną.

W przypadku urządzeń, jak podkreślał w swojej opinii EUNB, warunek „czegoś, co posiada tylko użytkownik" jest spełniony, jeśli istnieje wiarygodny (ang. *reliable*) sposób potwierdzenia władania tym urządzeniem przez użytkownika w momencie dokonywania transakcji. Za wiarygodny, godny zaufania uznaje się w tym przypadku taki, w którym następuje wygenerowanie bądź otrzymanie elementu dynamicznej weryfikacji na urządzeniu (European Banking Authority, 2018). Dopuszcza się w tym przypadku np. wygenerowanie jednorazowego hasła, wysłanie widomości SMS, w tym również specyficznego jego rodzaju, jakim jest wiadomość *push*. Za spełnienie wymogu w ramach elementu „posiadania" dla celów silnego uwierzytelniania klienta można uznać kartę SIM powiązaną z odpowiednim numerem telefonu komórkowego w połączeniu z potwierdzeniem osoby płatnika (walidacja) poprzez SMS. Najczęściej jako wypełniający cechy elementu posiadania wskazuje się telefon komórkowy, tzw. urządzenia ubieralne (*wearable device*) czy token. Zatem za spełniające wymogi EUNB uznaje się np. kartę lub urządze-

nie potwierdzone przez zeskanowanie z urządzenia zewnętrznego grafiki (kod QR, grafika photoTAN[6]) czy kartę potwierdzoną przez czytnik kart. Obowiązki w zakresie zapewnienia właściwych rozwiązań ciążą na dostawcy usług płatniczych (art. 97 ust. 3 PSD2).

Trzecim elementem jest kategoria określana mianem „cechy klienta". Opiera się na założeniu, że każdy ma cechy osobnicze różnicujące od pozostałych osób (cechy biometryczne), pozwalające na jednoznaczną identyfikację. Właściwość ta może zostać wykorzystana dla celów wymogów bezpieczeństwa w przypadku silnego uwierzytelniania (SCA), pod warunkiem że możliwe jest uchwycenie niepowtarzalności wyglądu, zachowań itd. przy zastosowaniu odpowiedniej technologii i zasadniczo w sposób niepodważalny identyfikować osobę płatnika. Mogą to być fizyczne dane biometryczne związane z właściwościami fizycznymi części ciała czy cechami fizjologicznymi (odcisk palców, wzory tęczówki, rozpoznawanie żył, głosu itd.), ale również, jak wskazano w opinii EUNB, cechy te mogą obejmować np. biometrię behawioralną, a więc identyfikacja może odbywać się w oparciu o wzorce działalności człowieka w interakcji między nim a urządzeniem (drżenie rąk, ruchy palcami, koordynacja ręka–oko, sposób pisania na klawiaturze[7]) w ramach stworzonego profilu (European Banking Authority, 2019). Jednocześnie motyw 6 preambuły RTS określa, że w tym przypadku istotna jest specyfikacja algorytmu, zabezpieczenia czytnika i wzorca biometrycznego. W praktyce podział metod identyfikacji między poszczególne kategorie (to znaczy określenie ich przynależności do kategorii „wiedza", „posiadanie" czy „cechy klienta") może nastręczać trudności. Mając na uwadze stanowisko EUNB, można wskazać, że do cech klienta zgodnych z SCA zalicza się uwierzytelnianie oparte na metodach skanowania odcisków palców, rozpoznawania głosu, biometrii układu żył, geometrii twarzy lub dłoni, skanowania siatkówki i tęczówki czy dynamice pisania na klawiaturze (European Banking Authority, 2019, s. 5). Natomiast stosowanie do uwierzytelniania tzw. zapamiętanej ścieżki przeciągania EUNB proponuje kwalifikować już jako element wiedzy (European Banking Authority, 2019, s. 5). Wybór techniki biometrycznej zależy od dostawcy, można jednak wskazać, że powinien on kierować się wieloma parametrami, jak m.in. jak najniższy współczynnik fałszywej akceptacji (np. wybór metod identyfikacji opartych na cechach ukrytych, które są trudniejsze do pozyskania, jak wzór naczyń krwionośnych) czy jej akceptowalność społeczna (zob. Lovisotto i in., 2017; Woszczyński, 2015; Mendyk-Krajewska, 2019, s. 35–46; Lott, 2018, s. 371–382).

Wymogi dotyczące urządzeń i oprogramowania powiązanych z elementami należącymi do kategorii „cechy klienta" określa art. 8 RTS. Istotna jest tu rola dostawców mających zapewnić, by prawdopodobieństwo uwierzytelnienia jako płatnika osób niepowołanych było bardzo niskie (art. 8 RTS).

Warto podkreślić, że innowacyjność tej części rynku finansowego powoduje, iż zakłada się dopuszczenie nowych rozwiązań technicznych, w szczególności tych, które będą ograniczać nie tylko istniejące, ale pojawiające się zagrożenia dla bezpieczeństwa płatności elektronicznych (motyw 2 preambuły RTS). Spośród wskazanych kategorii elementów uznaje się, że najbardziej innowacyjna i najszybciej rozwijająca się jest kategoria „cechy klienta" (European Banking Authority, 2019, s. 4).

Przechodząc do dalszych rozważań, trzeba powrócić do definicji legalnej silnego uwierzytelniania klienta. Jak wskazano w przypadku SCA, potwierdzenie deklarowanej tożsamości następuje poprzez odwoływanie się do określonych w przepisach kategorii, przy czym muszą one jednocześnie być niepowiązane ze sobą tak, iż nie wpływają wzajemnie na wiarygodność dokonywanej weryfikacji użytkownika. Wymóg niezależności elementów oznacza zatem, że w SCA uwierzytelnianie następuje w oparciu o zastosowanie co najmniej dwóch niezależnych elementów należących do różnych kategorii (European Banking Authority, 2018, pkt 33). Niezależność rozumiana jest tu jako brak takiego powiązania pomiędzy elementami, w którym próba płatności przez osobę nieuprawnioną z wykorzystaniem znajomości jednego z nich (np. w wyniku odkrycia danych) nie osłabia wiarygodności weryfikacji pozostałych. Szczegółowe wymogi w zakresie tzw. niezależności elementów precyzuje art. 9 RTS. W przepisach tych formułuje się zalecenia pod względem wymogów technicznych adresowanych do dostawców usług płatniczych. To oni zobligowani są do przyjęcia środków bezpieczeństwa, aby zmniejszyć ryzyko nadużyć, np. zobowiązani są do stosowania osobnych bezpiecznych środowisk uruchomieniowych za pośrednictwem oprogramowania zainstalowanego na urządzeniu wielofunkcyjnym.

Kod uwierzytelniający i dynamiczne łączenie jako środki bezpieczeństwa

RTS, określając i doprecyzowując wymagania dotyczące silnego uwierzytelniania klienta, w art. 4 stanowi, że dla SCA uwierzytelnienie nie tylko powinno się opierać na zastosowaniu do weryfikacji tożsamości klienta co najmniej dwóch elementów należących do kategorii identyfikujących użytkownika, ale także prowadzić do wygenerowania kodu uwierzytelniającego. Kod ten musi spełniać wymogi bezpieczeństwa opisane w motywach RTS (motyw 1 i 4 preambuły RTS), a szczegółowo unormowane w jego art. 4. RTS nie tworzy barier technicznych czy technologicznych w zakresie narzędzi stosowanych w procedurach uwierzytelniania, lecz wskazuje, że kod uwierzytelniający może opierać się na różnych metodach, które prowadzą do zapewnienia poufności i poprawnej weryfikacji tożsamości użytkownika. Przepisy dopuszczają rozwiązania oparte zarówno na generowaniu jednorazowych ciągów znaków wykorzystywanych jako tajny parametr (hasło) i potwierdzeniu przy jego/ich pomocy płatności czy podpisach cyfrowych, jak również innych metodach powiązanych z mechanizmami kryptograficznymi, o ile spełniają wymogi bezpieczeństwa. Te ostanie określa RTS opisowo, precyzując wymogi dotyczące zasad dokonywania transakcji przy użyciu kodu uwierzytelniającego oraz samego kodu. I tak, zgodnie z art. 4 ust. 2 RTS, kod można uznać za uwierzytelniający dla SCA, jeśli spełnia łącznie trzy wymogi: nie można go sfałszować, ujawniony nie może prowadzić do uzyskania informacji dotyczących elementów należących do kategorii identyfikują-

cych użytkownika (to jest „wiedza", „posiadanie" i „cechy klienta") oraz znajomość wcześniej wygenerowanego jakiegokolwiek innego kodu uwierzytelniającego nie umożliwia wygenerowania nowego kodu. RTS nie uściśla natomiast wymogów takich jak np. długość kodu uwierzytelniającego czy wielkość, która określa ilość informacji przypadających na wiadomość wysłaną przez źródło[8]. Rozporządzenie delegowane stanowi także o innych warunkach bezpieczeństwa płatności, określając: zasady przyjęcia kodu uwierzytelniającego (akceptowany jest tylko raz), maksymalny czas na dokonanie płatności (5 minut) czy graniczną wartość dozwolonych, następujących po sobie nieudanych prób uwierzytelnienia (5 prób w określonym okresie).

Wymogi określone w art. 5 RTS dotyczą natomiast dynamicznego łączenia. Obecnie obowiązujące przepisy wymagają swego rodzaju responsywności połączenia, to jest zdolności reakcji systemu operacyjnego tylko po otrzymaniu sygnału od płatnika, który miał możliwość sprawdzenia danych transakcyjnych. W ramach dynamicznego łączenia wypełnienie wymogów bezpieczeństwa następuje, jeśli spełniony jest każdy z następujących warunków: płatnik powiadomiony został o kwocie transakcji płatniczej oraz o odbiorcy; nastąpiło przypisanie wygenerowanego kodu uwierzytelniającego do kwoty transakcji płatniczej oraz do odbiorcy, które płatnik zaakceptował podczas inicjowania transakcji; przyjęty przez dostawcę usług płatniczych kod uwierzytelniający odpowiada pierwotnej, konkretnej kwocie transakcji płatniczej oraz tożsamości odbiorcy, które płatnik zaakceptował; a także by wszelkie zmiany zarówno kwoty, jak również danych odbiorcy skutkowały unieważnieniem wygenerowanego kodu uwierzytelniającego. Dostawcy usług płatniczych zobowiązani zostali, by zapewnić — na wszystkich etapach uwierzytelniania — takim elementom jak kwota transakcji i dane odbiorcy, informacje wyświetlane płatnikowi: poufność, autentyczność i integralność. Takie rozwiązania mają przede wszystkim eliminować ryzyko oszustw polegających na zmianie szczegółów transakcji po jej uwierzytelnieniu (przeciwdziałanie tzw. atakom *man-in-the-middle*).

Podsumowanie

Przedstawiona analiza prowadzi do kilku istotnych wniosków. Przede wszystkim potwierdza szczególny charakter prawa rynku usług płatniczych, które jako wyjątkowo silnie powiązane z innowacjami technicznymi ulega technologizacji. Skutkiem tego zjawiska jest to, że właściwa ochrona klienta wymaga sprostania specyficznym wyzwaniom w zakresie wykładni i stosowania prawa wynikających z przenoszenia na poziom normatywny i regulacyjny opisu rozwiązań inżynieryjnych, informatycznych, biometrycznych itd. Prawodawca czy regulator stosują m.in. siatkę pojęciową właściwą dla dyscyplin technicznych związaną niejednokrotnie z technikami informatycznymi (określenia: „kod uwierzytelniający", „dane uwierzytelniające", „dynamiczne łączenie transakcji", „bezpieczne środowiska uruchomieniowe"). W przypadku SCA, jak wykazano, może to prowadzić np. do niewłaściwej klasyfikacji przez dostawcę usług płatniczych przynależności określonych rozwiązań technicznych do jednej z kategorii „wiedza", „posiadanie", „cechy klienta", co może powodować naruszenie zasad uwierzytelniania w oparciu o co najmniej jeden z dwóch elementów należących do odrębnych kategorii.

Z punktu widzenia klienta jedna z podstawowych zasad świadczenia usług płatniczych zapewniająca bezpieczeństwo płatności — tj. zasada, że użytkownik musi udowodnić swoją tożsamość — została wzmocniona. Koncepcja SCA oparta jest m.in. na stosowaniu uwierzytelniania wieloczynnikowego, co ma utrudniać nadużycia związane z identyfikacją deklarowanej tożsamości i nieuprawnionym dostępem, w tym różnego rodzaju tzw. oszustwa płatnicze. Niemniej jednak wprowadzając nowe rozwiązania, należy mieć również na uwadze preferencje klientów. Dla nauk prawnych przydatne i interesujące są badania w zakresie gotowości technologicznej ludzi — zarówno społeczeństwa, jak również poszczególnych jednostek (Parasuraman, 2000, s. 307–320). Mogą oni być nieufnie nastawieni do stosowania nowych technologii, ponieważ nie są gotowi lub chętni do poddania się weryfikacji według obowiązujących reguł, co skutkować może rezygnacją z korzystania z usług np. odstąpienie od dokonania zakupu on-line. Jednocześnie współcześnie konsumenci w coraz większym stopniu oczekują, że płatności dokonywane będą szybko, bezpiecznie i przy zastosowaniu prostych w użyciu rozwiązań. Postrzeganie możliwości dokonania płatności przy spełnieniu tych warunków odgrywa fundamentalną rolę w rozwoju płatności. Wprowadzenie SCA może, zwłaszcza w pierwszym okresie obowiązywania przepisów, rodzić zagrożenia dla reputacji usługodawców, gdy proces realizacji transakcji, które wcześniej przebiegały bezproblemowo, zostanie zakłócony na skutek niedostosowania do SCA.

Na koniec należy też wspomnieć, że zakres stosowania rozwiązań PSD2 zależy m.in. od waluty i położenia geograficznego uczestników, co sprawia, że może nastąpić zróżnicowanie poziomu bezpieczeństwa płatności w odniesieniu do różnych transakcji dokonywanych przez klientów. Nie we wszystkich państwach udało się też dotrzymać daty określonej w PSD2, czego przyczyną jest złożoność wymogów i brak przygotowania, przy jednoczesnym potencjalnym znaczącym wpływie na konsumentów. Wprowadzenie rozwiązań przewidzianych w zakresie SCA musi być dokonywane w sposób bezpieczny dla rynku, zatem wskazane czynniki wymuszają przy wdrażaniu SCA odstępstwa od początkowo przyjętych terminów.

[1] PSD1 weszła w życie 25.12.2007 r., natomiast data implementacji wyznaczona została na 1.11.2009 r.

[2] Jest to rozporządzenie delegowane Komisji (UE) 2018/389 z 27.11.2017 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 komunikacji (Dz.Urz. UE L 69, s. 23), dalej RTS.

[3] W przypadku Wielkiej Brytanii pełna zgodność ma zostać osiągnięta do 14.03.2021, zob. Fiscal Conduct Authority, 2019.

[4] Zob. *European Banking Authority*. (2019), s. 4 oraz Komunikat KNF z 19.08.2019 r. w sprawie silnego uwierzytelniania klienta w przypadku niektórych form płatności przy użyciu instrumentów płatniczych, www.knf.gov.pl (27.11.2019).

[5] Szerzej na temat różnych definicji słowa „uwierzytelnianie" zob. np. T. Mielnicki, F. Wołowski, M. Grajek, P. Popis, 2013, s. 12–14.

[6] Na przykład bez aplikacji photoTAN od września nie można korzystać z bankowości internetowej Deutsche Banku. Aplikację tę stosuje też Commerzbank.

[7] Na ogromny potencjał tego rodzaju danych i ich wykorzystania do uwierzytelniania wskazuje się w praktyce i literaturze przedmiotu, zob. np. Antala, Zsolt Szabó, 2016, s. 862–869, Mendyk-Krajewska, 2018, s. 117–126.

[8] W kwestii uznania, jak długość kodu uwierzytelniającego wpływa na spełnienie wymogów, RTS wypowiadał się EBA — zob. Q&A 4053; https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4053 (27.11.2019).

Bibliografia

Antala, M., Zsolt Szabó, L. (2016). Biometric authentication based on touchscreen swipe patterns, *Procedia Technology 2016*, (22), 862–869. https://doi.org/10.1016/j.protcy.2016.01.061

Byrski, J. (2017). Consumer Protection under Directive 2015/2366 on Payment Services in the Internal Market — Selected Issues. *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, (8), 25–42. https://doi.org/10.15678/znuek.2017.0968.0802

European Banking Authority. (2014). Final Guidelines on the security of internet payments, EBA/GL/2014/12_Rev. European Banking Authority. https://eba.europa.eu/sites/default/documents/files/documents/10180/934179/f27bf266-580a-4ad0-aaec-59ce52286af0/EBA-GL-2014-12%20%28Guidelines%20on%20the%20security%20of%20internet%20payments%29_Rev1.pdf?retry=1 (27.11.2019).

European Banking Authority. (2018). Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, EBA-Op-2018-04, https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf (27.11.2019).

European Banking Authority. (2019). *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*. https://eba.europa. eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf (27.11.2019).

European Central Bank. (2013). *Recommendations for the Security of Internet Payments. Final Version After Public Consultation*. European Centraln Bank.

Fedorowicz, M., Zalcewicz, A. (2019). An Analysis of EBA Soft Law on the Payment Services Market. *Przegląd Ustawodawstwa Gospodarczego*, (1), 2–7.

Fiscal Conduct Authority. (2019). *FCA agrees plan for a phased implementation of Strong Customer Authentication*. https://www.fca.org.uk/news/press-releases/fca-agrees-plan-phased-implementation-strong-customer-authentication (27.11.2019).

Lott, D. (2018). Biometrics: Modernising customer authentication for financial services and payments. *Journal of Payments Strategy & Systems*, *12* (4), 371–382.

Lovisotto, G., Malik, R., Sluganovic, I., Roeschlin, M., Trueman, P., Martinovic, I. (2017). *Mobile Biometrics in Financial Services: A Five Factor Framework*. Oxford: Department of Computer Science. University of Oxford. http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services. pdf (27.11.2019).

Mendyk-Krajewska, T. (2018). Techniki uwierzytelniania biometrycznego dla realizacji usług drogą elektroniczną. *Ekonomiczne Problemy Usług*, (2), 117–126.

Mendyk-Krajewska, T. (2019). Biometryczne metody sprawdzania tożsamości w nowych zastosowaniach. *Rocznik Kolegium Analiz Ekonomicznych*, (54), 35–47. https://doi.org/10.18276/epu.2018.131/2-11

Mielnicki, T., Wołowski, F., Grajek, M., Popis, P. (red.). (2013). *Identyfikacja i uwierzytelnianie w usługach elektronicznych*. Warszawa: Związek Banków Polskich.

Parasuraman, P. (2000). Technology readiness index (TRI): A Multiple-Item Scale to Measure Readiness to Embrace New Technologies. *Journal of Service Research*, *2*(4), 307–320. https://doi.org/10.1177/109467050024001

Regnard-Weinrabe, B., Finlayson-Brown, J. (2019). Adapting to a changing payments landscape [w:] J. Madir (red.), *FinTech: Law and Regulation* (22–48). Cheltenham: Edward Elgar Publishing. https://doi.org/10.4337/9781788979023.00014

Woszczyński, T. (red.). (2015). *Biometria w bankowości — kluczowe aspekty*. Warszawa: Związek Banków Polskich.