Jakub Jan Szczerbowski
University of Lodz, Poland
jakub.szczerbowski@wpia.uni.lodz.pl
ORCID iD: https://orcid.org/0000-0002-2168-0741

DOI: 10.13166/JMS/139592
JOURNAL OF MODERN SCIENCE TOM 1/46/2021, S. 257–268

Liability of the payment service provider for the unauthorized payment transaction – comments on the basis of the Polish implementation of PSD2

Odpowiedzialność dostawcy usługi płatniczej za nieautoryzowaną transakcję płatniczą – uwagi na gruncie polskiej implementacji PSD2

Abstract

The purpose of this text is to discuss the interpretation of the provisions on the payment service provider's obligation to refund regarding unauthorized payment transactions. The subject of the research are the provisions of the Payment Services Act implementing the PSD2 directive in Poland. As part of the research, the formal-dogmatic method was applied. The result of the research is to propose an interpretation of the provisions governing the obligation to return the amount of unauthorized payment transactions to the payer. As part of the results, it was found that, due to the purpose of the legislation, as indicated in its wording and the recitals of the Directive, the obligation to return will be borne by the payer's supplier in principle, except in the event of fraud, intent or gross negligence on the part of the payer. As regards the problem of the burden of proof, a derogation from the general rule resulting from the provisions of the Civil Code consists in shifting the burden of proving that the transaction has been authorized to the supplier.

Streszczenie

Celem niniejszego tekstu jest wykładnia przepisów dotyczących obowiązku zwrotu ciążącego na dostawcach usług płatniczych, który dotyczy nieautoryzowanych transakcji płatniczych. Przedmiotem badań są przepisy ustawy o usługach płatniczych stanowiące implementację dyrektywy PSD2. W ramach badań zastosowano metodę formalno-dogmatyczną. Efektem badań jest zaproponowanie wykładni przepisów regulujących obowiązek zwrotu kwoty nieautoryzowanych transakcji płatniczych na rzecz płatnika. W ramach wyników ustalono, że ze względu na cel przyświecający przepisom, wynikający z ich brzmienia oraz motywów dyrektywy, obowiązek zwrotu będzie obciążał co do zasady dostawcę płatnika, wyjąwszy przypadek oszustwa, umyślności lub rażącego niedbalstwa po stronie płatnika. W zakresie problematyki ciężaru dowodu odstępstwo od ogólnej zasady wynikającej z przepisów kodeksu cywilnego polega na przeniesieniu na dostawcę ciężaru wykazania, że transakcja została autoryzowana.

Keywords: *unauthorised payment transaction, PSD2, payment institution, payment services, authentication*.

Słowa kluczowe: *nieautoryzowana transakcja płatnicza, PSD2, instytucja płatnicza, usługi płatnicze, uwierzytelnienie*.

Wprowadzenie

Problematyka nieautoryzowanych transakcji płatniczych regulowana jest na gruncie krajowego porządku prawnego przez Ustawę z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz.U. z 2020 r. poz. 794 ze zm., dalej: u.u.p.), implementującą Dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającą dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającą dyrektywę 2007/64/WE (Dz.U. UE. L. z 2015 r. Nr 337, str. 35 ze zm., dalej: PSD2). Implementacja PSD2 do porządków krajowych, jak się wskazuje w literaturze, napotyka trudności (por. Zunzunegui, 2020; Bani i in., 2021). W kontekście implementowanych rozwiązań toczy się w literaturze dyskusja na temat efektywności rozkładu odpowiedzialności za nieautoryzowane transakcje płatnicze (Harris, 2008; Ricks, 2016; Sommer, 2008) oraz przyszłości modeli płatności w obrocie z udziałem konsumentów (Burge, 2015; Conti-Brown, Wishnick, 2020).

Poprzez nieautoryzowaną transakcję płatniczą należy rozumieć taką transakcję, na którą płatnik nie wyraził zgody. Rozumienie takie wynika z wykładni przepisu art. 40 ust. 1 u.u.p. *a contrario*, która definiuje transakcję płatniczą autoryzowaną jako taką, na której wykonanie płatnik wyraził zgodę w sposób przewidziany w umowie pomiędzy płatnikiem a jego dostawcą. Pojęcie transakcji autoryzowanej jest więc na gruncie PSD2 odmienne niż w poprzednio obowiązującej dyrektywie (por. Wyżykowski, 2019, s. 102). Wykonanie zatem przez dostawcę usług płatniczych transakcji, na którą płatnik nie wyraził zgody, wymaga odpowiedniego uregulowania w przepisach prawa. Przepisy te regulują stopień swobody, w jakim strony mogą umownie określać sposób autoryzacji transakcji, przesłanki odpowiedzialności dostawcy usług płatniczych oraz przesłanki tę odpowiedzialność wyłączające. Omawiane przepisy mają w znaczącej części charakter bezwzględnie obowiązujący jedynie w relacjach z konsumentami, natomiast w relacjach pomiędzy przedsiębiorcami strony mogą umową wyłączyć ich obowiązywanie (por., art. 33 u.u.p.). Centralnym tematem niniejszego tekstu jest zakres i przesłanki wykonywania obowiązku dostawcy płatnika uregulowanego w przepisach art. 46 u.u.p., polegającego na zwrocie płatnikowi kwoty nieautoryzowanej transakcji albo na przywróceniu rachunku płatniczego do takiego stanu, jakby nieautoryzowana transakcja nie miała miejsca. W ramach omawianej problematyki konieczne jest zatem ustalenie znaczenia pojęcia transakcji nieautoryzowanej oraz omówienie przesłanek aktualizujących i wyłączających przedmiotowy obowiązek zwrotu.

Autoryzacja i uwierzytelnienie transakcji

Na gruncie u.u.p. dokonano rozróżnienia pomiędzy pojęciami uwierzytelnienia i autoryzacji. Uwierzytelnienie zostało zdefiniowane na gruncie PSD2 jako „procedur[a] umożliwiając[a] dostawcy usług płatniczych weryfikację tożsamości użytkownika usług płatniczych lub ważności stosowania konkretnego instrumentu płatniczego, łącznie ze stosowaniem indywidualnych danych uwierzytelniających tego użytkownika". Uwierzytelnienie należy więc traktować jako zespół czynności o charakterze faktycznym, które służą potwierdzeniu tożsamości płatnika.

Preferowanym sposobem uwierzytelnienia jest silne uwierzytelnienia klienta (uregulowane szczegółowo w Rozporządzeniu Delegowanym Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniającym 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), które polega na stosowaniu co najmniej dwóch środków należących do jednej z trzech kategorii: coś, co wie wyłącznie użytkownik (wiedza), coś, co posiada wyłącznie użytkownik (posiadanie) oraz coś, czym użytkownik jest (cechy klienta) (Leżoń, 2019, s. 33). Środki te mają być niezależne w taki sposób, że naruszenie jednego z nich nie osłabia skuteczności pozostałych, w szczególności jeżeli którykolwiek z tych elementów jest stosowany w urządzeniu wielofunkcyjnym, czyli w urządzaniu takim jak tablet lub telefon komórkowy. Uwierzytelnienie traktowane jest jako silne, gdy wymagane jest użycie przynajmniej dwóch z ww. elementów.

Powszechnie stosowanymi środkami silnego uwierzytelnienia są ciągi znaków używane jako ustalone hasło (wiedza) używane w połączeniu z hasłami jednorazowymi przekazywanymi za pośrednictwem telefonu lub aplikacji mobilnej (posiadanie). Dyskusyjne jest, czy stosowanie wiadomości tekstowych przesyłanych na telefon stanowi poprawne stosowanie przepisów PSD2 i u.u.p., ponieważ w takim przypadku może zachodzić wątpliwość co do spełnienia przez dostawcę obowiązku wynikającego z przepisu art. 43 ust. 1 u.p.p., zgodnie z którym dostawca wydający instrument płatniczy jest obowiązany do zapewnienia, że dane uwierzytelniające nie są dostępne dla osób innych niż użytkownik. Należy więc stwierdzić, że dostawca korzystający z dostarczanej przez osobę trzecią (dostawcę usług telekomunikacyjnych) usługi przesyłania w sposób niezaszyfrowany danych uwierzytelniających ponosi ryzyko takiego działania. Powstaje tu pytanie o możliwość odmiennego ukształtowania rozkładu ryzyka w umowie z konsumentem. Mając na uwadze, że przeniesienie ryzyka korzystania przez dostawcę z usługi podmiotu trzeciego na konsumenta może prowadzić do zniweczenia ochronnego celu przepisów art. 46 u.u.p., postanowienia umowne tego typu należy uznać za niedozwolone.

Stosowanie przez dostawcę silnego uwierzytelnienia użytkownika jest obowiązkowe w przypadkach wskazanych w przepisie art. 32i ust. 1 u.u.p.,

tj. w przypadku dostępu do rachunku w trybie online, inicjowania elektronicznej transakcji płatniczej lub przeprowadzania za pomocą kanału zdalnego czynności, która może wiązać się z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innych nadużyć. Ta ostatnia przesłanka nakłada na dostawcę usług płatniczych obowiązek oceny ryzyka związanego z usługami płatniczymi i odpowiedniego stosowania silnego uwierzytelnienia.

Dokonując rozróżnienia pomiędzy uwierzytelnieniem i autoryzacją transakcji, należy się skupić na istocie tych dwóch pojęć. W doktrynie wskazuje się, że uwierzytelnienie „polega na zweryfikowaniu jego [płatnika] tożsamości lub ważności stosowania instrumentu płatniczego" (Wyżykowski, 2019, s. 107); takie stanowisko pozwala łatwo odróżnić uwierzytelnienie od autoryzacji transakcji, której istotą jest wyrażenie przez płatnika zgody na wykonanie transakcji płatniczej. Pojęcie autoryzacji, chociaż nie jest tożsame z oświadczeniem woli płatnika, pozostaje z nim w pewnym związku – przeciwnie do pojęcia uwierzytelnienia, które z oświadczeniem woli nie ma nic wspólnego, będąc jedynie zdarzeniem faktycznym podobnym do okazania dowodu osobistego przy czynnościach dokonywanych przy osobistej obecności stron. Nie każde oświadczenie woli płatnika będzie jednak stanowiło autoryzację; chodzi tu o przypadki, w których oświadczenie nie odpowiada wymogom ustanowionym w umowie pomiędzy płatnikiem a dostawcą usług płatniczych.

Mając na uwadze powyższe zagadnienia, należy uznać, że do nieautoryzowanej transakcji płatniczej dochodzi wówczas, gdy pomimo braku zgody płatnika dokonywana jest transakcja płatnicza na jego rachunek.

Zakres i przesłanki odpowiedzialności dostawcy usługi płatniczej

Zgodnie z dyspozycją przepisu art. 46 ust. 1 u.u.p. wystąpienie nieautoryzowanej transakcji płatniczej aktualizuje po stronie dostawcy płatnika obowiązek zwrotu kwoty tej transakcji, a w przypadku rachunku płatniczego – obowiązek przywrócenia tego rachunku do takiego stanu, jaki miałby miejsce, gdyby nieautoryzowana transakcja nie wystąpiła. Ograniczeniem przedmiotowym (kwotowym) odpowiedzialności dostawcy płatnika są transakcje

do wysokości odpowiadającej wartości 50 EUR, będące skutkiem posłużenia się utraconym przez płatnika albo skradzionym mu instrumentem płatniczym lub przywłaszczenia instrumentu płatniczego, a płatnik miał możliwość stwierdzenia utraty, kradzieży lub przywłaszczenia instrumentu płatniczego i nie była ona spowodowana działaniem lub zaniechaniem ze strony pracownika, agenta lub oddziału dostawcy płatnika (por. art. 46 ust. 2 i 2a u.u.p.). Pewne trudności interpretacyjne może powodować użycie terminów „utrata", „kradzież" i „przywłaszczenie", ponieważ na gruncie języka polskiego nazwy „utrata" i „kradzież" oraz „utrata" i „przywłaszczenie" mają krzyżujące się zakresy – innymi słowy, zawsze w przypadku kradzieży albo przywłaszczenia instrumentu płatniczego dochodzi także do jego utraty. Z tego względu w literaturze proponuje się, aby wykładać termin „utrata" w art. 46 ust. 2a pkt 2 w sposób szeroki (Wyżykowski, 2019, s. 106). Pogląd ten zasługuje na aprobatę i odpowiada celom stawianym przez PSD2.

Na płatniku ciąży obowiązek powiadomienia dostawcy o wystąpieniu nieautoryzowanej transakcji płatniczej niezwłocznie (art. 44 ust. 1 u.u.p.). Uchybienie temu obowiązkowi może stanowić przesłankę negatywnej oceny staranności płatnika. Zwłoka płatnika w powiadomieniu dostawcy o wystąpieniu nieautoryzowanej transakcji nie wywołuje skutku w postaci wygaśnięcia prawa, o ile nie zostanie przekroczony termin 13 miesięcy. Przesłanką odpowiedzialności dostawcy płatnika jest zatem dokonanie przez płatnika powiadomienia w terminie 13 miesięcy od dnia wystąpienia nieautoryzowanej transakcji płatniczej (art. 46 ust. 1 w zw. z art. 44 ust. 2 u.u.p.). Termin ten ma charakter zawity, niedokonanie przez płatnika powiadomienia skutkuje wygaśnięciem roszczenia. Obowiązek zwrotu obciążający dostawcę płatnika powinien zostać zrealizowany niezwłocznie. Także w tym przypadku ustawa przewiduje termin, z którym związane są dalej idące skutki prawne, a mianowicie termin jednego dnia roboczego (tzw. D+1). Termin ten jest tak krótki, że trudno jest mówić o zwłoce, w przypadku gdy zwrot nie następuje niezwłocznie, ale nadal z zachowaniem terminu D+1. Skutkiem uchybienia terminowi zwrotu jest opóźnienie dłużnika (dostawcy płatnika) ze spełnieniem świadczenia pieniężnego, co rodzi po stronie płatnika roszczenie o zapłatę odsetek za czas opóźnienia oraz roszczenie o naprawienie szkody na zasadach ogólnych. Celem ustanowienia tak krótkiego terminu jest zapewnienie płynności płatnika.

Okoliczności wyłączające odpowiedzialność instytucji płatniczej

Obowiązek zwrotu wynikający z art. 46 ust. 1 u.u.p. nie ma charakteru bezwzględnego; ustawodawca przewidział szereg okoliczności wyłączających odpowiedzialność dostawcy, mając na uwadze, że nieograniczona odpowiedzialność dostawcy (np. względem płatnika nieuczciwego) prowadziłaby do nieracjonalnego podwyższenia kosztów działalności dostawców, być może nawet do poziomu zupełniej nieopłacalności. Jak już wcześniej wspominano, odpowiedzialność dostawcy jest wyłączona (roszczenie płatnika wygasa) w przypadku niewykonania przez płatnika obowiązku z przepisu art. 44 ust. 2 u.u.p.

Okolicznością ograniczającą obowiązek zwrotu jest użyte w przepisie art. 46 ust. 1 u.u.p. sformułowanie „[…] z wyjątkiem przypadku gdy dostawca płatnika ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo, i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw […]". Fragment ten budzi wątpliwości interpretacyjne. Przede wszystkim wymaga wyjaśnienia, czy oszustwo w rozumieniu tego przepisu ma zostać dokonane przez płatnika, czy też może być to inna osoba. Prezentowane są odmienne stanowiska, pierwsze dopuszcza wąskie rozumienie oznaczające oszustwo dokonane przez płatnika, a także z udziałem płatnika (*Analiza Rzecznika Finansowego. Nieautoryzowane transakcje – zasady i główne problemy*, 2019, s. 11), drugie stanowisko nie ogranicza „oszustwa" do oszustwa płatnika (Wyżykowski, 2019, s. 114). Przyjęcie drugiego stanowiska, dopuszczającego zwolnienie się dostawcy z odpowiedzialności w przypadku oszustwa dokonanego przez osobę trzecią, jest o tyle problematyczne, że rodzi niespójność aksjologiczną. W znaczącej liczbie przypadków transakcji nieautoryzowanych dochodzi do oszustw płatniczych dokonywanych przez osoby trzecie – przepisy PSD2 oraz u.u.p. mają natomiast na celu stworzenie odpowiednich zachęt do podniesienia poziomu ochrony przed tego typu naruszeniami (por. Gawron, 2019, s. 55). Przyjęcie zatem koncepcji, że dokonane przez dowolną osobę oszustwo płatnicze zwalnia dostawcę z odpowiedzialności, ogranicza prawne zachęty do podnoszenia poziomu ochrony przez dostawców usług płatniczych; nie oznacza to oczywiście, że takich zachęt nie będzie w ogóle,

mogą one nadal występować np. w sferze wizerunkowej. Ponadto przyjęcie drugiej koncepcji pozostaje w kolizji z przepisem art. 46 ust. 3 u.u.p., przewidującym odpowiedzialność płatnika działającego umyślnie lub rażąco niedbale; *a contrario* płatnik działający starannie powinien pozostawać pod ochroną ustawy, w przypadku gdy osoba trzecia dopuści się oszustwa płatniczego. Mając na względzie powyższe uwagi, należy przychylić się do pierwszego stanowiska, czyli wykładani terminu „oszustwo" jako oszustwa płatnika. Kolejnym elementem koniecznym do zwolnienia dostawcy z odpowiedzialności jest zawiadomienie przez dostawcę organów powołanych do ścigania przestępstw o popełnieniu przez płatnika przestępstwa w formie pisemnej. Do zwolnienia z odpowiedzialności nie wystarczy więc zawiadomienie o oszustwie w formie innej niż pisemna ani zawiadomienie w formie pisemnej pochodzące od innego podmiotu. Istotą tego uregulowania jest nadanie odpowiedniej wagi temu zawiadomieniu, w szczególności mając na uwadze odpowiedzialność karną za fałszywe oskarżenie (art. 234 k.k.) oraz fałszywe zawiadomienie o przestępstwie (art. 248 k.k.). Z uwagi na brzmienie przepisu art. 65(1) w zw. art. 78(1) § 2 k.c. dopuszczalne jest także przekazanie do organu powołanego do ścigania przestępstw informacji opatrzonej kwalifikowanym podpisem elektronicznym.

Przesłanką zwalniającą dostawcę z odpowiedzialności za nieautoryzowaną transakcję płatniczą jest doprowadzenie do niej przez płatnika umyślnie albo fakt, iż jest ona wynikiem umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków określonych w art. 42 u.u.p., takich jak: 1) korzystanie z instrumentu płatniczego zgodnie z umową ramową, 2) zgłaszanie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu, 3) podejmowanie niezbędnych środków służących zapobieżeniu naruszenia indywidualnych danych uwierzytelniających. Należy przy tym podkreślić, że naruszenie obowiązków będące wynikiem zachowania płatnika niekwalifikowanego jako rażąco niedbałe albo umyślne nie prowadzi do zwolnienia dostawcy płatnika z odpowiedzialności za nieautoryzowaną transakcję płatniczą. Taka regulacja zasługuje na aprobatę, albowiem stopień skomplikowania urządzeń technicznych służących do

obsługi transakcji płatniczych może uniemożliwiać pełne wykonanie obowiązków umownych przez płatnika. Z tego względu zgodne z wartościami systemowymi jest takie ukształtowanie obowiązków, aby dopiero rażące niedbalstwo rodziło odpowiedzialność po stronie płatnika. Posłużenie się przez ustawodawcę klauzulą generalną rażącego niedbalstwa pozwala na dostosowanie wzorca zachowania zarówno do zmieniających się w czasie możliwości technicznych i ewoluującej przeciętnej świadomości użytkowników w tym zakresie, jak i do warunków osobistych płatnika, które mogą wpływać na ocenę staranności jego zachowania.

Ciężar udowodnienia faktów

Kluczowym zagadnieniem dotyczącym ochrony cywilnoprawnej jest problematyka ciężaru udowodnienia faktów, zwana także ciężarem dowodu. W przypadku sporu pomiędzy płatnikiem i dostawcą płatnika obowiązki dowodowe stron uregulowane są przede wszystkim zasadą ogólną wynikającą z przepisu art. 6 k.c., od której przepisy u.u.p. przewidują pewne odstępstwa. Przeniesienie ciężaru dowodu na dostawcę dotyczy, zgodnie z art. 45 ust. 1. u.u.p., faktu autoryzowania i prawidłowego zapisania transakcji w systemie służącym do obsługi transakcji płatniczych oraz faktu braku wpływu na nią awarii technicznej lub innego rodzaju usterki. Nie ulega wątpliwości, że postawiony przed dostawcą standard może prowadzić do trudności dowodowych.

Dostrzeżono to także w opracowaniach, wskazując alternatywne możliwości wykładni zwrotu „[n]a dostawcy użytkownika spoczywa ciężar udowodnienia, że transakcja płatnicza została autoryzowana i prawidłowo zapisana […]" poprzez traktowanie prawidłowego zapisu i braku awarii jako prawnego domniemania autoryzacji transakcji:

> [b]iorąc pod uwagę jednoznaczne brzmienie przepisów PSD1 i PSD2, należy przyjąć, że dowodami autoryzacji ze strony dostawcy – na gruncie art. 45 UUP – są następujące okoliczności: b) prawidłowy zapis w systemie służącym do obsługi transakcji płatniczych dostawcy, c) brak awarii technicznej (Związek Banków Polskich, 2018, s. 4).

Stanowisko takie zupełnie odwraca istotę przepisu art. 45 ust. 1 u.u.p., prowadząc do obniżenia wymogów w zakresie ciężaru dowodu po stronie dostawcy. Nie tylko stoi ono w sprzeczności z brzmieniem przepisu, który wskazuje wprost, na kim spoczywa ciężar udowodnienia autoryzacji transakcji, ale także zatraca sens tego przepisu, który dostrzega nierówność stron w zakresie dowodzenia faktów; wszakże to po stronie dostawcy pozostają wszelkie informacje związane z transakcją nieautoryzowaną, włącznie z informacjami historycznymi dotyczącymi innych nieautoryzowanych transakcji wykorzystujących tę samą podatność lub sposób działania (por. Lubowiecki, 2017), podczas gdy płatnik dysponuje jedynie informacją szczątkową – o wysokości transakcji nieautoryzowanej oraz rachunku, na jaki została przekazana. O ile wykazanie przez dostawcę autoryzacji transakcji może być utrudnione, o tyle wykazanie przez płatnika, że transakcji nie autoryzował, może okazać się niemożliwe. Mając więc na uwadze, że prawo należy interpretować przy założeniu racjonalności ustawodawcy (racjonalny ustawodawca nakłada na podmioty prawa obowiązki możliwe do spełnienia), należy przyjąć, że ciężar udowodnienia, że transakcja została autoryzowana, spoczywa na dostawcy.

Za taką interpretacją przemawia także brzmienie art. 45 ust. 2 u.u.p., podwyższającego standard dowodu, jakiemu musi sprostać dostawca, poprzez uznanie za niewystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana albo że płatnik umyślnie albo wskutek rażącego niedbalstwa doprowadził do nieautoryzowanej transakcji płatniczej albo umyślnie bądź wskutek rażącego niedbalstwa dopuścił się naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 u.u.p., wyłącznie poprzez wykazanie użycia instrumentu płatniczego. Przepis ten jest zgodny z przepisem artykułu 72 PSD2 („[…w]here a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 69 […]"). Należy także zauważyć, że w przypadkach nieautoryzo-

wanych transakcji płatniczych wykazanie, że transakcja była autoryzowana, będzie niemożliwe ze względu na brak zgody płatnika w stanie faktycznym sprawy. Wysoce wątpliwe jest więc wykładanie przepisu w sposób pozwalający na zastąpienie zgody płatnika zapisami w systemie i brakiem awarii technicznej. Pomimo to dostawcy nadal przysługują zarzuty wyłączające jego odpowiedzialność, ciężar wykazania których będzie spoczywał na nim – zgodnie z ogólną regułą rozkładu ciężaru dowodu.

Podsumowanie

Celem komentowanych przepisów prawa jest zapewnienie ochrony klientów dostawców usług płatniczych, a w szczególności konsumentów w obszarze nieautoryzowanych transakcji płatniczych. Ocena taka może wynikać nie tylko z brzmienia przepisów u.u.p., ale także z motywów PSD2 (por. motywy 4, 5, 6, 8, 70, 71, 73, 76). Ustalenie celu regulacji pozwala na prawidłową interpretację, która rozważa zachęty powstające po każdej ze stron. W przypadku gdy wykładania językowa prowadzi do odkodowania norm zachęcających do niezapewnienia wysokiego poziomu bezpieczeństwa czy wręcz ignorowania zagrożeń przez strony w zakresie swojej strefy wpływów – zasadne jest odejście od wykładni językowej na rzecz wykładni celowościowej. Obok zapewnienia wysokiego poziomu bezpieczeństwa celem przedmiotowych przepisów jest zapewnienie bezpieczeństwa indywidualnym konsumentom, w tym ochrony przed niewypłacalnością – chociażby przejściową – wynikającą z uszczerbku na ich majątku powstałego wskutek nieautoryzowanej transakcji płatniczej. Te dwa cele pozostają w relacji wzajemnego wzmacniania – obowiązek zwrotu kwoty nieautoryzowanej transakcji płatniczej w terminie D+1 pozwala na zapewnienie płynności konsumenta *in concreto*, a jego perspektywa *in abstracto* wywołuje presję ekonomiczną w kierunku stosowania odpowiednich zabezpieczeń technicznych, w tym dostosowywania ich do potrzeb poszczególnych kategorii klientów, a także podkreśla rolę samych instytucji płatniczych oraz ich zrzeszeń w pełnieniu funkcji edukacyjnej, która dla poziomu ochrony ma niebagatelne znaczenie.

Bibliografia

Bani, E., De Stasio, V., Sciarrone Alibrandi, A. (2021). *L'attuazione della Seconda Direttiva sui servizi di pagamento e „Open Banking"*, Sestante: Bergamo University Press.

Burge, M.E. (2015). *Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law*, „Hastings Law Journal", No. 67, s. 1493.

Conti-Brown, P., Wishnick, D.A. (2020). *Private Markets, Public Options, and the Payment System*, „Yale Journal on Regulation", No. 37, s. 380.

Gawron, O. (2019). *Otoczenie regulacyjne sektora fintech na przykładzie dyrektywy PSD2 i wybranych ustaw krajowych*, http://dspace.uni.lodz.pl:8080/xmlui/handle/11089/32122 (dostęp: 15.05.2021).

Harris, S.L. (2008). *Introduction to Rethinking Payments Law*, „Chicago-Kent Law Review", No. 83, s. 477.

Leżoń, K. (2019). *Otwarta bankowość w* świetle *wymogów dyrektywy DSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech* (I), Komisja Nadzoru Finansowego.

Lubowiecki, D. (2017). *Prawno-kryminalistyczna problematyka phishingu, ze szczególnym uwzględnieniem środowiska bankowości internetowej*, „Kwartalnik Prawo – Społeczeństwo – Ekonomia", nr 9(1), s. 30–43.

Ricks, M. (2016). *Safety First: The Deceptive Allure of Full Reserve Banking*, „University of Chicago Law Review Online", No. 83, s. 113.

Rzecznik Finansowy. (2019). *Analiza Rzecznika Finansowego. Nieautoryzowane transakcje – zasady i główne problemy*.

Sommer, J.H. (2008). *Where Is the Economic Analysis of Payment Law*, „Chicago-Kent Law Review", No. 83, s. 751.

Wyżykowski, B. (2019). *Odpowiedzialność za nieautoryzowane transakcje płatnicze – wybrane zagadnienia wynikające z implementacji PSD2*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny (iKAR)", nr 8(8), s. 101–116.

Zunzunegui, F. (2020). *Spain's Implementation of PSD2*, „Revista de Derecho Del Mercado Financiero", Noviembre 2020.

Związek Banków Polskich. (2018). *Wyjaśnienia interpretacyjne i rekomendacje sektora bankowego w zakresie przepisów: 1) ustawy z dnia 10 maja 2018 r. – O zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw (UZUP), 2) dyrektywy Parlamentu Europejskiego I Rady (UE) 2015/2366 z dnia 25 listopada 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 (PSD2) oraz 3) ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (UUP)*, https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/pisma-urzedowe/wyjasnienia-interpretacyjne-i-rekomendacje-sektora-185098062 (dostęp: 15.05.2021).