Rozdział 26

Michał Nowakowski

OD OTWARTEJ BANKOWOŚCI DO OTWARTYCH FINANSÓW – OGRANICZENIA OTWARTEJ BANKOWOŚCI Z PERSPEKTYWY PRAWNO-REGULACYJNEJ

Sektor finansowy od wielu lat przechodzi istotne przeobrażenia, zarówno w sferze stricte prawno-regulacyjnej (w tym ostrożnościowej), jak i cyfrowej. Wydarzenia ostatnich lata, w tym w szczególności pandemia SARS-CoV-2 wpłynęły w istotny sposób na dynamikę transformacji produktów i usług finansowych, jak również same instytucje finansowe[709], np. w sferze cyfryzacji[710]. Klienci stają się bardziej wymagający zarówno w zakresie kanałów dystrybucji produktów i usług[711], ale także samej ich konstrukcji[712], oczekując większej personalizacji, niskich kosztów oraz łatwości dostępu (*frictionless*) i znaczenie lepszych doświadczeń, tzw. *user experience*[713]. Stawia to przed instytucjami finansowym wiele wyzwań o charakterze biznesowym, prawno-regulacyjnym oraz operacyjnym. Oczekiwania stawiane przez klientów wymagają bowiem dokonywania zmian w modelach biznesowych, poszukiwania nowych rozwiązań i kanałów dystrybucji, jak również równoważenia ryzyk.

Szczególnie interesująca w kontekście usług finansowych jest tzw. zaawansowana analityka danych oraz Big Data[714], często traktowana na równi z szeroko

---

709 IFC, *The Early Impact of COVID-19 on financial institutions. Insights from a survey of IFC financial institution clients*, https://www.ifc.org/wps/wcm/connect/587d57c6-74dd--4efb-90cc-5dec218fd00e/COVID-19+Impact+on+FI+Survey+2020+-+5-11--2021_FINAL+REVIEW.pdf?MOD=AJPERES&CVID=nBz3kgr: dostęp: 8.01.2022 r.

710 E. Feyen, J. Frost, L. Gambacorta, H. Natarajan, M. Saal, *Fintech and the digital transformation of financial services: implications for market structure and public policy*, BIS Papers No 117, July 2021, s. 46.

711 EBA, *Report on the use of digital platforms in the EU banking and payments sector*, EBA/REP/2021/26, September 2021, s. 8.

712 Ł. Gębski, *The Impact of the Crisis Triggered by the COVID-19 Pandemic and the Actions of Regulators on the Consumer Finance Market in Poland and Other European Union Countries*, Risks 9: 102, s. 2, https://www.mdpi.com/2227-9091/9/6/102/pdf: dostęp: 8.01.2022 r.

713 C.M. Barbu, D.L. Florea, D. -C. Dabija, M.C.R. Barbu, *Customer Experience in Fintech*, J. Theor. Appl. Electron. Commer. Res. 2021, 16, 1415–1433, https://www.mdpi.com/0718-1876/16/5/80/pdf: dostęp: 8.01.2022 r. Tutaj tzw. doświadczenie użytkownika jest definiowane jako konstrukt psychologiczny, który zawiera subiektywną reakcję klienta na interakcję z firmą, jej markami, usługami i/lub produktami.

714 EBA, *Report on Big Data and Advanced Analytics*, EBA/REP/2020/01, January 2020, https://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf: dostęp: 8.01.2022 r.

rozumianą sztuczną inteligencją[715], która w sposób istotny zwiększa możliwości indywidualizacji produktów i usług finansowych w oparciu o dane, biometrię behawioralną[716]. Połączenie tych elementów może mieć istotne znaczenie dla klientów, jak i samych instytucji, choć wymaga to uwzględnienia szeregu aspektów dotyczących samych danych, w tym przede wszystkim możliwości ich pozyskiwania oraz przetwarzania.

Pewną próbą uwolnienia danych finansowych, które mogą posłużyć do tworzenia bardziej spersonalizowanych jest otwarta bankowość[717], której ramy prawne w Unii Europejskiej wyznacza dyrektywa PSD2[718] oraz Rozporządzenie 2018/389[719], choć należy jednocześnie zaznaczyć, że nie jest to zarazem pierwszy przejaw wykorzystania danych z rachunków płatniczych przez tzw. podmioty trzecie (*Third-Party Providers* – TPP)[720]. Przepisy obu aktów prawnych, jak również liczne akty o miękkim charakterze (o czym w dalszej części opracowania), stanowią od 14 września 2019 r. podstawę realizacji koncepcji otwartej bankowości opartej o obowiązek udostępniania poprzez tzw. interfejsy dostępowe (*Application Programming Interfaces* – API) wybranych danych finansowych przez podmioty do tego zobowiązane (m.in. banki). Dane te mogą być – za zgodą użytkownika – wykorzystywane m.in. do realizacji usługi dostępu do informacji o rachunku płatniczym.

Choć założenia otwartej bankowości były i są słuszne, to jednak przepisy[721] oraz koncepcja realizacji okazały się na tyle niedopracowane i nieprzemyślane (choć to nie jedyny powód ograniczonego rozwoju), że dzisiaj trudno mówić

---

715 Więcej na ten temat w: M. Nowakowski, K. Waliszewski, *Sztuczna inteligencja i algorytmy w służbie finansów osobistych. Perspektywa prawno-ekonomiczna*, Przegląd Ustawodawstwa Gospodarczego, 08/2021.

716 L. Banga, S. Pillai, *Impact of Behavioural Biometrics on Mobile Banking System*, Series r. 1964, 062109, 2021, s. 2–3.

717 Próbę zdefiniowania otwartej bankowości podejmują m.in. P. Laplante oraz N. Kshetri, którzy proponują, aby traktować ją jako specjalny rodzaj finansowego ekosystemu, który umożliwia podmiotom trzecim z obszaru usług finansowych otwarty dostęp do bankowości detalicznej, transakcji oraz innych danych finansowych pochodzących od banków i niebankowych instytucji finansowych, które są udostępniane poprzez interfejsy dostępowe. P. Laplante, N. Kshetri, *Open Banking: Definition and Description*, Computing's Economics, October 2021, s. 123.

718 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, Dz. Urz. UE z 2015 r., L-337/35.

719 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 komunikacji, Dz. Urz. UE z 2018 r., L-69/23.

720 Mowa tutaj o metodzie tzw. *screen scrapingu*, o którym mowa chociażby w piśmie Komisji Nadzoru Finansowego skierowanym do Sejmu w 2015 r., https://orka2.sejm.gov.pl/INT7.nsf/klucz/088552EF/%24FILE/i33434-01.pdf: dostęp: 9.01.2022 r.

721 Dotyczy to nie tylko samych przepisów odnoszących się do usług płatniczych, ale także tych które dotykają sfery ochrony prywatności i danych osobowych. EDPB, *Guidelines 06/*

o prawdziwej rewolucji w zakresie wykorzystania danych finansowych, chociażby na potrzeby finansów osobistych (i to niezależnie od rosnącej liczby podmiotów FinTech[722]). Wydaje się, że jest to niejako konsekwencja braku „efektu zachęty"[723] po stronie instytucji obowiązanych do udostępniania danych, jak również pewnej nierównowagi obowiązków i odpowiedzialności po stronie poszczególnych „aktorów" realizujących usługi w ramach otwartej bankowości.

Pewne mankamenty otwartej bankowości zostały dostrzeżone także przez Komisję Europejską, która w 2020 r. wskazała w dokumencie w sprawie strategii dla UE w zakresie finansów cyfrowych[724] na potrzebę stworzenia ram w zakresie otwartych finansów. Zgodnie z założeniami Komisji do połowy 2022 r. ma zostać złożony wniosek ustawodawczy, zaś do 2024 r. UE powinna już dysponować odpowiednimi rozwiązaniami w tym zakresie. Warto zwrócić tutaj uwagę, że przez 3 lata nie udało się uzyskać satysfakcjonującego poziomu efektywności interfejsów dostępowych, które umożliwiają swobodne realizowanie usług przez TPP[725]. To oczywiście nie jedyna przeszkoda, bowiem niewątpliwie znaczenie ma tutaj także swoista niechęć klientów banków do dzielenia się informacjami z TPP, o czym szerzej w dalszej części opracowania.

Niewątpliwie jednak otwarta bankowość stanowi kamień milowy dla rozwoju innowacyjnych rozwiązań z obszaru finansów, choć wyzwań, m.in. prawno-regulacyjnych, w tym kontekście jest jeszcze wiele. Próbą dokonania prawdziwej rewolucji w sferze finansowej jest wspomniana już koncepcja otwartych finansów, która w połączeniu przykładowo z rozwojem platform cyfrowych[726], może otworzyć drogę do bardziej spersonalizowanych finansów, co jest wskazywane często jak główny trend w sektorze finansowym[727]. Otwarte finanse mają na celu stwo-

---

2020 on the interplay of the Second Payment Services Directive and the GDPR, 15 grudnia 2020 r.

722 M. Polasik, A. Huterska, R. Iftikhar, S. Mikula, *The impact of PSD2 on the functioning of the retail payment market*, Journal of Economic Behaviour and Organization, No. 178, 2020, https://reader.elsevier.com/reader/sd/pii/S0167268120302328?token=289F3DE95E05DB7DE2A641346AA7E74B7C5779969D2BD45E8BD9EE6D4DB80CE4CF99C5E40041EDD55EAFE2579083868F&originRegion=eu-west-1&originCreation=20220114090625: dostęp: 14.01.2022 r.

723 Podobnie K. O'Leary, T. Nagle, P. O'Really (et.al.), *The Sustainable Value of Open Banking: Insights from an Open Data Lens*, Proceedings of the 54th Hawaii International Conference on System Sciences, 2021, s. 5898.

724 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0591&from=EN: dostęp: 9.01.2022 r.

725 EBA, *Opinion of the European Banking Authority on supervisory actions to ensure the removal of obstacles to account access under PSD2*, EBA/Op/2021/02, 18 February 2021, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963372/Opinion%20on%20supervisory%20actions%20for%20removal%20of%20obstacles%20to%20account%20access%20under%20PSD2.pdf: dostęp: 14.01.2022 r.

726 P. Sironi, Banks and Fintechs, *Banks and Fintech on Platform Economies. Contextual and Conscious Banking*, Wiley 2022.

727 Deloitte, *The future of retail banking. The hyper-personalisation imperative*, November 2020.

rzenie warunków do pozyskiwania, przetwarzania i dostarczania produktów i usług finansowych o bardziej zindywidualizowanym i kompleksowym charakterze.

Celem niniejszego rozdziału jest wskazanie na pewne słabe punkty prawno-regulacyjne w zakresie otwartej bankowości, jak również zaproponowanie możliwych kierunków zmian, które mają szczególne znaczenie dla rozwoju otwartych gospodarek opartych o dane. Z tego względu aspekty historyczne dotyczące przyjęcia dyrektywy PSD2 oraz implementującej ją ustawy o usługach płatniczych zostaną ograniczone do niezbędnego minimum. Jednocześnie podkreślić należy, że niniejsze opracowanie nie dotyka przyszłych – możliwych – wariantów rozwoju finansów cyfrowych, które mogą obejmować nie tylko rozwój otwartych finansów, ale także pewne połączenie finansów zdecentralizowanych z tradycyjnymi. Jest to zagadnienie jednak daleko wykraczające poza ramy niniejszego opracowania, choć warto zwrócić na nie uwagę również w kontekście oceny otwartej bankowości.

1. Otwarta bankowość w dyrektywie PSD2 oraz Rozporządzeniu 2018/389

Pierwsze założenia prawne zmierzające do urzeczywistnienia koncepcji otwartej bankowości zostały wyrażone w dyrektywie PSD2, która jednak ze swej istoty nie wprowadziła jeszcze takich rozwiązań pozwalających na jej implementację. Te pojawiły się dopiero wraz z uchwaleniem na podstawie art. 98 dyrektywy PSD2 i wejściem w życie Rozporządzenia 2018/389 ustanawiającego wspólne i bezpieczne otwarte standardy komunikacji niezbędne do wymiany informacji (danych) w ramach otwartej bankowości. W Polsce pewne elementy dotyczące przedmiotowego zagadnienia uwzględnione zostały w ustawie zmieniającej ustawę o usługach płatniczych[728], choć zakres „techniczny" materii pozostał w Rozporządzeniu 2018/389 oraz miękkich regulacjach mu towarzyszących, o czym w dalszej części opracowania.

Na całokształt ram prawnych otwartej bankowości składają się zasadniczo dwa elementy:

1. Nowe usługi wprowadzone przez dyrektywę PSD2[729], tj. usługa dostępu do informacji o rachunku płatniczym (AIS – *Account Information Service*) oraz usługa inicjowania płatności (PIS – *Payment Initation Services*) wraz wymogami dla dostawców je świadczących oraz
2. Obowiązki po stronie dostawców usług płatniczych prowadzących rachunek (w znacznej mierze banki) w zakresie posiadania i udostępniania interfejsów dostępowych API (*Application Programming Interface*)[730].

---

728 Ustawa z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw, Dz. U. z 2018 r., poz. 1075.

729 M. Grabowski, *Legal Aspects of "White-Label" Banking in the European, Polish and German Law*, Journal of Risk and Financial Management 14: 280, s. 7.

730 Tematyce wykorzystania tzw. API w bankowości poświęcony jest m.in. raport Banku Rozrachunków Międzynarodowych. BIS, *Report on open banking and application*

Połączenie tych elementów składa się niejako na możliwość zrealizowania koncepcji otwartej bankowości, przy zastrzeżeniu zgody użytkownika, którego dane lub środki dotyczy realizacja konkretnej usługi. W pewnym uproszczeniu można więc stwierdzić, że otwarta bankowość w rozumieniu pakietu PSD2 to realizacja niektórych usług finansowych w układzie użytkownik-dostawca zewnętrzny-podmiot „posiadające" dane finansowe użytkownika. Poprzez zastosowanie konkretnych narzędzi prawnych stało się możliwe dokonywanie wymiany wrażliwych danych oraz inicjowania płatności za pośrednictwem podmiotów, które dotychczas mogły polegać na konstrukcjach prawnych, które mogły budzić wątpliwości, jak np. wspomniany już screen-scraping.

Założenia prawne w tym zakresie zostały określone w art. 30-36 Rozporządzenia 2018/389 oraz (zasadniczo[731]) w dziale IIIB ustawy o usługach płatniczych. W szczególności art. 30 ust. 1 wskazuje, że dostawcy usług płatniczych prowadzący rachunku, którzy oferują płatnikowi rachunek płatniczych dostępny za pośrednictwem internetu, posiadają co najmniej jeden interfejs spełniający każdy z wymogów[732]:

1. Dostawcy usługi AIS, dostawcy usługi PIS oraz dostawcy wydający instrumenty płatnicze oparte na karcie są w stanie zidentyfikować się wobec dostawcy prowadzącego rachunek.
2. Dostawcy usługi AI są w stanie bezpiecznie komunikować się w celu wystąpienia o informacje i uzyskania informacji na temat jednego wyznaczonego rachunku płatniczego lub większej ich liczby i powiązanych transakcji płatniczych.
3. Dostawcy usługi PIS są w stanie bezpiecznie komunikować się w celu zainicjowania zlecenia płatniczego z rachunku płatniczego płatnika i uzyskania wszystkich informacji dotyczących zainicjowania transakcji płatniczej oraz wszystkich informacji dotyczących realizacji transakcji płatniczej, do których dostęp mają dostawcy prowadzący rachunek.

Oczywiście wymogi te mają charakter podstawowy, natomiast w dalszych przepisach znajdują się bardziej szczegółowe wymogi dotyczące m.in. obowiązku udostępniania dokumentacji technicznej czy wymogów dla tzw. specjalnych interfejsów dostępowych. Przepisy Rozporządzenia 2018/389 wymagają także „specjalnego" procesu identyfikacji TPP z użyciem certyfikatów wydawanych na podstawie Rozporządzenia 910/2014[733], które zawierają m.in. informacje doty-

---

programming interfaces November 2019, https://www.bis.org/bcbs/publ/d486.pdf: dostęp: 24.01.2022 r.

731 W praktyce wiele przepisów jest zlokalizowanych w całej ustawie, w szczególności w odniesieniu do odpowiedzialności podmiotów za właściwą realizację konkretnych usług.

732 Od strony technicznej funkcjonowanie otwartej bankowości w ramach pakietu PSD2 dobrze opisują T. Wich, D. Nemmert, D. Huhlnein, *Towards secure and standard-compliant implementations of the PSD2 Directive* (w:) L. Fritsch et al. (red.), Open Identity Summit 2017, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017.

733 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do

czące posiadania statusu podmiotu nadzorowanego oraz zakresu świadczonych usług. Takie rozwiązanie, przynajmniej w pewnym zakresie, ma zapewnić, że realizacja usługi AIS oraz PIS odbywać się będzie jedynie za pośrednictwem upoważnionych do tego podmiotów. W praktyce jednak rozwiązanie to okazuje się nie do końca skuteczne, o czym w dalszej części rozdziału.

Istotne jest również podkreślenie, że cała komunikacja (wymiana danych) w ramach realizacji powyższych usług powinna odbywać się z zastosowaniem odpowiednich rozwiązań w zakresie bezpieczeństwa, m.in. z użyciem szyfrowania danych czy zabezpieczeń fizycznych, np. związanych z nieuprawnionym dostępem do indywidualnych danych uwierzytelniających. Określone zasady obowiązują także w odniesieniu do zakresu przekazywanych danych oraz stosowania środków awaryjnych, które mogą znaleźć zastosowanie w przypadku utraty funkcjonalności specjalnych interfejsów dostępowych.

Jednocześnie, wspomniane już przepisy art. 59q–59t ustawy o usługach płatniczych wprowadzają szczególne obowiązki po stronie podmiotów uczestniczących w realizacji tych usług[734]. Obowiązki te mają bardzo zróżnicowany charakter i odnoszą się przykładowo do konieczności zapewnienia bezpieczeństwa danych czy ograniczeń w zakresie pozyskiwania danych o charakterze szczególnie wrażliwym. Katalog ten jest oczywiście znacznie szerszy, ale ograniczony ramy opracowania nie pozwalają na przybliżenie wszystkich aspektów dotyczących tego zagadnienia.

Całokształt rozwiązań prawnych i regulacyjnych, w tym licznych wyjaśnień Europejskiego Urzędu Nadzoru Bankowego[735] oraz Urzędu Komisji Nadzoru Finansowego, składa się na praktyczne ramy rozwoju otwartej bankowości, której mankamenty zostaną przedstawione w kolejnym rozdziale.

2. Mankamenty otwartej bankowości z perspektywy prawno-regulacyjnej

Nadzieje związane z otwartą bankowością były znaczne, choć już po uchwaleniu dyrektywy PSD2 pojawiały się głosy o pewnych niejasnych jej aspektach, chociażby w odniesieniu do podziału odpowiedzialności pomiędzy poszczególne podmioty uczestniczące w realizacji usługi[736], ale także standaryzacji interfejsów dostępo-

transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, Dz. Urz. UE L-257/73.

734 Na konsekwencje wejścia w życie pakietu PSD2 w kontekście bezpieczeństwa danych klientów zwracają uwagę m.in. M. Hałasik-Kozajda, M. Olbryś, *Skutki implementacji dyrektywy o usługach płatniczych (PSD2)*, Bank i Kredyt 52(3), 2021, s. 292.

735 Przykładowo https://www.eba.europa.eu/regulation-and-policy/payment-services--and-electronic-money/eba-working-group-on-apis-under-psd2 : dostęp: 26.01.2022 r.

736 P. Valcke, N. Vandezande, N. van de Velde, *The Evolution of Thirt Party Payment Providers and Cryptocurrencies under the EU's Upcoming PSD2 and AML4*, SWIFT Institute Working Paper No. 2015-001, 23 September 2015, s. 70.

wych (w szczególności na poziomie unijnym) czy edukacji odbiorców rozwiązań opartych o otwartą bankowość[737]. P.T.J. Wolters oraz B.P.F. Jacobs wskazują nawet, że Rozporządzenie 2018/389 nieadekwatnie chroni dane użytkowników, a nawet może generować określone ryzyka w zakresie bezpieczeństwa[738], co w połączeniu z „nieszczelnymi" przepisami w zakresie odpowiedzialności (zarówno odszkodowawczej, jak i regulacyjnej), stawia pod znakiem zapytania poprawność implementacji pakietu PSD2.

Nie są to jednak jedyne mankamenty pakietu dla otwartej bankowości. Jednym z kluczowych zarzutów, jakie można postawić prawodawcy unijnemu przy wprowadzaniu pakietu PSD2 jest brak uwzględnienia zachęt dla instytucji zobowiązanych do otwierania swoich interfejsów dostępowych, które to zachęty mogłyby przyczynić się do zwiększenia zaangażowania i zainteresowania banków tworzeniem takich modeli, które wykraczałyby poza niezbędne minimum, a nawet doprowadziły do tworzenia swoistych bankowych platform (*bank marketplace*)[739]. Z drugiej strony nie wprowadzono także rozwiązań, które wpłynęłyby na zwiększenie zaufania potencjalnych klientów TPP, co mogłoby istotnie wpłynąć na rozwój szeroko rozumianej otwartej bankowości. Tworzenie takich zachęt na poziomie aktu legislacyjnego nie jest oczywiście zadaniem łatwym, ale nie niemożliwym.

2.1. Odpowiedzialność dostawców usług

Głównym powodem (abstrahując oczywiście od aspektów konkurencji[740]), dla którego banki niechętnie podchodzą do kwestii otwartego dostępu do danych są kwestie związane z ich odpowiedzialnością za ewentualne naruszenia w tym obszarze. Przykładowo, przepisy ustawy o usługach płatniczych wskazują, jakie obowiązki ciążą na dostawcy świadczącym usługę AIS, m.in. w zakresie wykorzystywania danych wyłącznie do celu realizacji usługi. Jednocześnie, w przypadku naruszenia tego obowiązku przepisy nie wskazują specyficznych rozwiązań prawnych co do odpowiedzialności. Innymi słowy, podmiot będzie mógł podlegać odpowiedzialności za naruszenia regulacyjne w trybie przewidzianym dla nadzoru KNF, odpowiedzialności za dane osobowe[741] (na zasadach wyznaczanych przez

---

737 M. Petrovic, *PSD2 Influence on Digital Banking Transformation – Banks' Perspective*, Journal of Process Management – New Technologies, International Vol. 8, No. 4, 2020, s. 3.

738 P.T.J. Wolters oraz B.P.F. Jacobs, *The security of access to accounts under the PSD2*, Computer Law & Security Review (35), 2019, s. 41.

739 P.-J. van de Venn, *'Mobile First' will become 'API First' — PSD2: Changing banking as we know it*, Journal of Digital Banking, Vol. 2, 2 2017, s. 172.

740 E. Jagodzińska-Komar, J. Grzywacz, *Rola interfejsu API w modelu otwartej bankowości*, Kolegium Zarządzania i Finansów. Zeszyt Naukowy 172, 2019, s. 48.

741 Jest to odrębne zagadnienie, które zostało opisane m.in. przez Europejską Radę Ochrony Danych. EDPB, Wytyczne 6/2020 w sprawie wzajemnych zależności między dyrektywą PSD2 a RODO, przyjęte 15 grudnia 2020 r., https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_pl.pdf : dostęp: 28.01.2022 r.

Rozporządzenie 2016/679[742]) oraz potencjalnej odpowiedzialności cywilnej – na zasadach ogólnych. Brak przepisów specyficznie odnoszących się do kwestii odpowiedzialności za dane pozyskiwane w ramach tej usługi, co wydaje się dość istotnym brakiem, zważywszy na rolę tych podmiotów oraz wartość przetwarzanych danych.

W przypadku usługi inicjowania płatności sytuacja kształtuje się nieco inaczej. Art. 46 ust. 1a uUP wyraźnie wskazuje, że gdy transakcja płatnicza jest inicjowana za pośrednictwem dostawcy świadczącego usługę PIS dostawca prowadzący rachunek niezwłocznie[743], nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, zwraca płatnikowi kwotę nieautoryzowanej transakcji płatniczej oraz, w stosownych przypadkach, przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza. Przepis art. 46 ust. 1b precyzuje, że w przypadku, gdy dostawca usługi PIS jest odpowiedzialny za dokonanie nieautoryzowanej transakcji (np. wskutek niedochowania obowiązków wynikających z ustawy), to na wniosek podmiotu, który wykonał transakcję, jest on obowiązany do rekompensaty (nie wpływa to na możliwość ustalenia dodatkowej odpowiedzialności dostawcy usługi PIS względem płatnikiem). W konsekwencji, to jednak podmiot realizujący transakcję odpowiada w pierwszej kolejności względem użytkownika nieautoryzowanej transakcji.

Powyższe przykłady wskazują na jedną istotną „wadę" pakietu PSD2 – nierównowagę praw i obowiązków podmiotów realizujących usługi PIS, AIS oraz COF (*Confirmation of Funds* – potwierdzenie dostępności środków). Dotyczy to nie tylko samej odpowiedzialności za dane czy transakcje nieautoryzowane, ale także wymogów o charakterze prawno-regulacyjnym w obszarze m.in. zarządzania ryzykiem czy bezpieczeństwa. Wiele z podmiotów, w tym dostawcy świadczący wyłącznie usługę dostępu do informacji o rachunku (jest to odrębna kategoria dostawców usług płatniczych), nie jest zobowiązanych do posiadania rozwiązań w powyższym obszarze na (takim samym) poziomie jak przykładowo banki, wobec których zastosowanie mają także liczne rekomendacje Urzędu Komisji Nadzoru Finansowego[744]. Rodzić to może więc słuszne obawy o bezpieczeństwo danych[745],

---

742 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE z 2016 r., L-119/1.

743 Więcej o problematyce nieautoryzowanych transakcji (w:) Rzecznik Finansowy, *Nieautoryzowane transakcje – zasady i główne problemy*, 18 czerwca 2019 r., https://rf.gov.pl/wp-content/uploads/2020/05/Nieautoryzowane_trasnsakcje_analiza-RF_2019.pdf : dostęp: 28.01.2022 r.

744 Przykładowo Rekomendacja H dotycząca kontroli wewnętrznej w bankach czy Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

745 Więcej (w:) I. Romānova, S. Grima, J. Spiteri, M. Kudinska, *The Payment Services Directive 2 and Competitiveness: The Perspective of European Fintech Companies*, European Research Studies Journal Volume XXI, Issue 2, 2018, s. 10.

choć nie zawsze są one uzasadnione. Ten stan może zmienić projektowane rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014[746] („DORA"), które w założeniu ma ustanowić jednolite wymogi w zakresie cyfrowej odporności operacyjnej, która zyskuje na znaczeniu wraz z rozwojem kanałów cyfrowych.

Należy w tym miejscu zauważyć jednak, że dzisiejsze rozwiązania, np. wspomniany już art. 46 ust. 1a powodują, że wszelkie ewentualne roszczenia za nieudaną transakcję kierowane będą w pierwszej kolejności do banku, który w układzie wprowadzonym dla usługi PIS jest *de facto* jedynie wykonawcą transakcji zainicjowanej przez podmiot trzeci. Ponosi więc on nie tylko finansowy uszczerbek (sam proces dochodzenia rekompensaty od TPP może być procesem długotrwałym), ale także reputacyjną szkodę związaną z oszukańczym działaniem innego podmiotu. Podobnie w przypadku usługi AIS istnieje ryzyko, że pomimo niezrealizowana jednego lub wielu obowiązków przez podmiot świadczący tą usługę, w przypadku zaistnienia sytuacji utraty danych lub ich niewłaściwego wykorzystania[747], roszczenie reklamacyjne klienta będzie w pierwszej kolejności kierowane do banku, który udostępnił dane, a nie samego TPP.

Pewnym zabezpieczeniem ewentualnej odpowiedzialności jest obowiązek posiadania przez podmioty świadczące usługi PIS oraz AIS odpowiedniego zabezpieczenia w formie umowy ubezpieczenia odpowiedzialności[748] cywilnej lub gwarancji bankowej, gwarancji ubezpieczeniowej lub innego zabezpieczenia roszczeń użytkownika (art. 61b, art. 117a ust. 3 uUP), choć szczególnie w odniesieniu do ubezpieczenia dla dostawców świadczących wyłączeniu usługę dostępu do informacji o rachunku wyzwanie stanowi samo pozyskanie takiego zabezpieczenia.

Ograniczone ramy opracowania nie pozwalają na bardziej szczegółowe omówienie zagadnienia, jednakże w tym miejscu warto jednak zwrócić uwagę, że rozwiązanie tego delikatnego problemu jest możliwe przy zastosowaniu stosunkowo prostych rozwiązań o charakterze prawnym (choć niewątpliwie muszą one być uzupełnione o edukację społeczeństwa). W odniesieniu do dostawców usługi PIS, jak i AIS, zasadnym wydaje się przykładowo wprowadzenie obowiązków wyraźnego informowania użytkowników o ryzykach związanych z usługą, jak i odpowiedzialności w tym zakresie. O ile część z tych wymagań wynika już wprost

---

746 https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020PC0595&from=EN : dostęp: 28.01.2022 r.

747 Na kluczowe znaczenie obszaru cyberbezpieczeństwa w ramach TPP wskazują m.in. A.W. Ng, B. K. B. Kwok, *Emergence of Fintech and cybersecurity in a global financial centre. Strategic approach by a regulator*, Journal of Financial Regulation and Compliance Vol. 25 No. 4, 2017, s. 426.

748 Wymogi w tym zakresie określa Rozporządzenie Ministra Finansów z dnia 31 lipca 2019 r. w sprawie minimalnej sumy gwarancyjnej ubezpieczenia, sumy gwarancji bankowej, sumy gwarancji ubezpieczeniowej lub wartości innego zabezpieczenia roszczeń użytkownika, o których mowa w art. 117a ust. 3 ustawy o usługach płatniczych, Dz. U. z 2019 r., poz. 1458.

z przepisów odnoszących się do obowiązków informacyjnych, w tym w zakresie zawartości umowy ramowej, to bardziej wyraźny i przejrzysty obowiązek komunikacyjny byłby tutaj zasadny. Może to oczywiście przynieść ten skutek, że użytkownicy będą mniej chętni do realizacji usług za pośrednictwem TPP, jednakże zwiększyć to może poziom bezpieczeństwa tych usług, a także wyeliminować część wyzwań stojących przed otwartą bankowością. W odniesieniu do dostawców świadczących wyłącznie usługę AIS konieczne wydaje się również wyraźne określenie zasad odpowiedzialności „za dane", tak aby nie budziło wątpliwości co stanowi podstawę prawną takiej odpowiedzialności. Dziś wątpliwości może bowiem budzić to czy zastosowanie mają przepisy o ochronie danych osobowych czy też ustawy o usługach płatniczych, a być może oba. Nie są to oczywiście rozwiązania doskonałe, które gwarantują, że m.in. banki otworzą się bardziej na korzyści płynące z pakietu PSD2, ale większa przejrzystość z pewnością jest tutaj pożądana.

Istotnym wątkiem jest również dostępność ubezpieczeń i gwarancji, które umożliwiają prowadzenie działalności. Brak możliwości zakupu takiego produktu przez podmioty świadczące usługi PIS oraz AIS powoduje, że ich możliwości stają się ograniczone. W tym zakresie postulowanym rozwiązaniem mogłoby być stworzenie swoistego funduszu ubezpieczeniowego, który nie tylko mógłby udzielać stosownych ubezpieczeń, ale także pokrywać ewentualne szkody (w skrajnych przypadkach). Z pewnością zwiększyłoby to poziom zaufania do takich dostawców, szczególnie jeżeli połączone byłoby to z obowiązkiem wyraźnego informowania o takim zabezpieczeniu.

2.2. Odmowa dostępu TPP

W tym miejscu należy zwrócić uwagę na jeszcze jedną kwestię, która dotyczy bezpośrednio dostawców świadczących usługę dostępu do rachunku (najczęściej banków). Art. 41 ust. 5 uUP stanowi pewną furtkę dla takich podmiotów do odmowy[749] TPP realizacji usługi AIS lub PIS. Może to jednak nastąpić jedynie z obiektywnie uzasadnionych i należycie udokumentowanych przyczyn związanych z nieuprawnionym lub nielegalnym dostępem do rachunku. W takim przypadku (bank) jest zobowiązany poinformować płatnika o odmowie i jej przyczynach w ściśle określonych terminach. Jednocześnie (bank) jest zobowiązany zgłosić do KNF zaistnienie takiego incydentu. Przepis ten rzeczywiście może stanowić podstawę do odmowy realizacji usługi, ale nie uwzględnia on samej specyfiki (technicznej) tych usług.

749 Zwrócić należy jednocześnie uwagę, że jednym z głównych wątków stanowiących źródło sporu pomiędzy bankami oraz TPP jest kwestia tzw. przeszkód w realizacji usług w ramach pakietu PSD2. Europejski Urząd Nadzoru Bankowego regularnie publikuje wyjaśnienia w tym zakresie, a w połowie 2020 r. wydał nawet stosowną opinię. EBA, *Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC*, EBA/OP/2020/10, 4 June 2020.

Po pierwsze, proces realizacji usługi można sprowadzić do następujących kroków:

1. Żądanie i zgoda użytkownika na realizację usługi PIS lub AIS.
2. Przekazanie żądania użytkownika oraz identyfikacja TPP z użyciem certyfikatu eIDAS wobec systemu transakcyjnego.
3. Proces uwierzytelniania w systemie transakcyjnym.
4. Zwrot informacji lub wykonanie transakcji.

Jest to oczywiście pewne uproszczenie schematu działania tych usług. Istotne jest jednak to, że realizacja tych usług następuję, a przynajmniej powinna, praktycznie natychmiastowo (niezauważalnie dla użytkownika, co jest konsekwencją zastosowania m.in. art. 32 ust. 1 Rozporządzenia 2018/389), choć oczywiście niektóre podmioty stosują kontrowersyjne techniki ograniczania poziomu dostępności i efektywności tych interfejsów[750]. Ze wspomnianego już przepisu art. 41 ust. 5 wynika zaś, że odmowa dostępu może nastąpić **z obiektywnie uzasadnionych i należycie udokumentowanych przyczyn związanych z nieuprawnionym lub nielegalnym dostępem do rachunku.**

Pojawia się więc zasadnicze pytanie w jaki sposób dostawca świadczący usługę dostępu do rachunku mógłby zrealizować założenia powyższego przepisu. Wymagałoby to wdrożenia rozwiązań, które w czasie rzeczywistym i natychmiastowo pozwalają na zidentyfikowanie potencjalnie podejrzanej transakcji lub żądania. W przypadku usług świadczonych jednak przez podmioty trzecie może być to znacznie utrudnione, chociażby ze względu na brak bezpośredniej interakcji (z wyjątkiem procesu uwierzytelnienia) na etapie składania zlecenia. Problemem jest również określenie, czym są obiektywnie uzasadnione przyczyn, jak również w którym momencie powinno nastąpić ich udokumentowanie. Jest to przykład przepisów, który może stanowić istotną barierę dla rozwoju sektora innowacji finansowych w Polsce[751].

Jednym z przypadków, w których może nastąpić realizacja usługi w sposób nieuprawniony, jest sytuacja, w której organ nadzoru cofnął TPP stosowne zezwolenie na prowadzenie działalności, np. w charakterze krajowej instytucji płatniczej, natomiast zmiana ta nie jest jeszcze uwidoczniona w samym certyfikacie eIDAS[752],

---

750 Na konieczność niezwłocznego usunięcia przeszkód w dostępie przez TPP do specjalnych interfejsów dostępowych zwraca uwagę m.in. Europejski Urząd Nadzoru Bankowego. EBA, *Opinion of the European Banking Authority on supervisory actions to ensure the removal of obstacles to account access under PSD2*, EBA/Op/2021/02, 18 February 2021, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963372/Opinion%20on%20supervisory%20actions%20for%20removal%20of%20obstacles%20to%20account%20access%20under%20PSD2.pdf : dostęp: 28.01.2022 r.

751 Na nieprecyzyjne i niespójne przepisy w obszarze innowacji finansowych wskazują m.in. A. Kliber, B. Będowska-Sójka, A. Rutkowska, K. Świerczyńska, *Triggers and Obstacles to the Development of the FinTech Sector in Poland*, Risks 9: 30, February 2021, s. 6.

752 Jednym z istotnych wyzwań po stronie regulatorów jest aktualizacja rejestrów zezwoleń czy rejestracji podmiotów podlegających ich nadzorowi. Jeżeli nie są one aktualizowane w czasie rzeczywistym i z chwilą np. cofnięcia zezwolenia (innym aspektem jest tutaj

który stanowi podstawę identyfikacji[753] takiego podmiotu względem np. banku. Bank może posiłkować się publicznie dostępnymi rejestrami, jak np. Europejskiego Urzędu Nadzoru Bankowego, ale i to jest rozwiązaniem zawodnym, bowiem dane tam wskazane mogą nie odpowiadać rzeczywistości[754]. Jeżeli jednak bank lub inny podmiot realizujący dyspozycję TPP ma podejrzenie, że zachodzi przesłanka uzasadniająca przyjęcie, że podmiot nie jest już uprawniony do świadczenia usługi PIS lub AIS, to teoretycznie powinien mieć on możliwość do wstrzymania realizacji żądania.

Patrząc jednak przez pryzmat wspomnianego przepisu sprawa nie jest tak oczywista. Niedookreśloność pojęcia „obiektywnych przyczyn związanych z nieuprawnionym lub nielegalnym dostępem do rachunku płatniczego przez takiego dostawcę, w tym nieuprawnionym zainicjowaniem transakcji płatniczej" powoduje, że instytucja odmawiająca realizacji żądania musi być niemalże pewna swoich racji. M. Torończak słusznie wskazuje także, że „(k)atalog przyczyn umożliwiających odmowę dostępu do rachunku płatniczego jest zamknięty - obejmuje wyłącznie nieuprawniony lub nielegalny dostęp do tego rachunku, w tym nieuprawnione zainicjowanie transakcji płatniczej"[755], co zawęża katalog potencjalnych sytuacji dopuszczających taką odmowę[756]. O tym więc czy dostawca usługi rachunku jest upoważniony do odmowy wykonania żądania decydować będzie m.in. to czy mamy do czynienia z potencjalnie nieautoryzowaną transakcją[757], czy też dostępem do rachunku dokonanym w sposób nieuprawniony, np. wskutek braku zgody użytkownika na pozyskanie tych danych.

Wspomniana już sytuacja posłużenia się przez TPP ważnym certyfikatem, który jednak powinien utracić swoją ważność np. na skutek cofnięcia zezwolenia przez właściwy organ, rodzi jednak poważne wątpliwości. Z punktu widzenia

---

ocena tego w którym momencie decyzja staje się ostateczna), to istnieje stan niezgodności treści takiego rejestru ze stanem faktycznym.

753 Aspekty identyfikacji TPP z użyciem tych rozwiązań zostały opisane m.in. przez Europejski Urząd Nadzoru Bankowego. EBA, *Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC*, EBA-Op-2018-7, 10 December 2018 r.

754 Informacje znajdujące się we wspomnianym rejestrze Europejskiego Urzędu Nadzoru Bankowego są gromadzone na bazie danych przekazywanych przez krajowe organy nadzoru, a ponadto – jak wskazują stosowne zastrzeżenia – są to dane, które nie mają „mocy prawnej". Podmioty powinny kierować się danymi zawartymi w krajowych rejestrach. Dostęp do rejestru: https://euclid.eba.europa.eu/register/ : dostęp: 28.01.2022 r.

755 M. Torończak, *Nakazywanie przez KNF przyznania dostępu do rachunku płatniczego*, Monitor Prawa Bankowego 2019, nr 5, s. 103-112.

756 Jest to o tyle istotne, że zgodnie z art. 41 ust. 6-7 takie przypadki podlegają kontroli ze strony KNF.

757 Ograniczone ramy niniejszego opracowania nie pozwalają na przybliżenie zagadnienia nieautoryzowanych transakcji, ale należy wskazać, że budzi ono wiele wątpliwości zarówno ze strony organów (m.in. Rzecznik Finansowy), jak i samego sektora bankowego. Kwestia ta była przedmiotem wielu orzeczeń sądowych, m.in. wyroku Sądu Apelacyjnego w Warszawie z dnia 19 lipca 2018 r. (I ACa 348/17) czy wyroku Sądu Apelacyjnego w Warszawie VI ACa 217/17.

Rozporządzenia 2018/389 oraz uUP w takiej sytuacji zasadniczo TPP działa zgodnie z przepisami, szczególnie jeżeli zgoda użytkownika została wyrażona w sposób prawidłowy. Wątpliwy jest jedynie stan faktyczny, na który bank nie ma wpływu i może (powinien) polegać na poprawnym certyfikacie eIDAS. W związku z tym pojawia się kolejne pytanie – czy jeżeli bank w jakikolwiek sposób wszedł w posiadanie dodatkowych informacji i ma podejrzenie co do stanu prawnego TPP – to czy będzie to obiektywna przyczyna? Jeżeli tak, to w jaki sposób „odpowiednie" udokumentować tą przyczynę. Wątpliwości budzi także sama kwalifikacja takiego dostępu do rachunku – czy jest ona nieuprawnionym lub nielegalnym dostępem?

Rozstrzygnięcie takich wątpliwości następuje więc w trybie weryfikacji zasadności przez KNF lub inny organ nadzoru, jednakże po stronie samego podmiotu uprawnionego do odmowy żądania budzi to stan pewnej niepewności, która w połączenie z ryzykiem odpowiedzialności cywilnej, jak i regulacyjnej, może skutkować niechęcią banków do zarówno badania legalności żądań, jak i samej odmowy, nawet w przypadku powzięcia uzasadnionych podejrzeń.

Rozwiązaniem tego stanu niepewności byłoby doprecyzowanie przepisów w tym zakresie, w tym w kontekście usprawnienie komunikacji na linii organ nadzoru – wydawca certyfikatu eIDAS dla TPP oraz wyraźne określenie obowiązku natychmiastowego przekazania informacji o cofnięciu lub zawieszeniu zezwolenia w celu unieważnienia certyfikatu. W samym art. 41 ust. 5 uUP zasadnym wydaje się wprowadzenie pewnych zmian, np. poprzez wskazanie, że taka odmowa może nastąpić w wyniku uzasadnionych podejrzeń, że żądanie TPP może naruszać prawa użytkownika lub osób trzecich, w szczególności jest nieuprawnione lub nastąpiło z naruszeniem przepisów prawa. Jednocześnie zasadne wydaje się doprecyzowanie, że udokumentowanie podejrzeń powinno nastąpić niezwłocznie po odmowie dostępu. Jednocześnie wydaje się, że korzystnym rozwiązaniem byłoby wyraźne wskazanie, że jeżeli realizacją żądania przez np. bank nastąpiła na skutek przekazania poprawnych informacji, w tym certyfikatu i zgody, to taki podmiot nie ponosi odpowiedzialności za ewentualne szkody powstałe na skutek nieuprawnionego lub nielegalnego działania.

2.3. Dostęp (tylko) do rachunku płatniczego

Kolejnym wątkiem, który należy poruszyć w kontekście pakietu PSD2 jest wąski zakres danych (choć uwagę można i rozciągnąć na usługę PIS), które zgodnie z art. 59s. ust. 1 mogą być pobierane wyłącznie z rachunku płatniczego. Zgodnie z literalnym brzmienie przepisu realizacja usługi AIS może odbywać się jedynie w odniesieniu do informacji zgromadzonych na rachunkach płatniczych. Definicja takiego rachunku została wskazana m.in. w art. 2 pkt 25) uUP zgodnie z którym za rachunek płatniczy uważamy rachunek prowadzony dla jednego lub większej liczby użytkowników służący do wykonywania transakcji płatniczych, przy czym przez taki rachunek rozumiemy także m.in. wybrane rachunki bankowe. Definicja ta nie jest do końca klarowna i wątpliwości na tym tle powstawały już wcześniej.

W jednym z wyroków Trybunał Sprawiedliwości (UE) stwierdził, że rachunek, z jakiego transakcje płatnicze nie mogą być przeprowadzane bezpośrednio, lecz do ich dokonania konieczne jest skorzystanie z rachunku pośredniego, nie może być uważany za rachunek płatniczy[758]. W orzeczeniu tym Trybunał odmówił takiego statusu chociażby rachunkowi oszczędnościowemu[759], choć zwrócić uwagę należy, że analogiczna uwaga może być poczyniona względem np. rachunków (kart) kredytowych, w tym kredytów hipotecznych. Wprowadza to istotne ograniczenie w zakresie całokształtu stanu finansów użytkownika. Jeżeli dodatkowo spojrzymy na art. 36 ust. 1 pkt a) Rozporządzenia 2018/389, to okaże się także, że i zakres informacji z rachunków płatniczych podlega ograniczeniom.

Zgodnie z treścią tego przepisu dostawcy usług płatniczych prowadzący rachunki przekazują dostawcom świadczącym usługę dostępu do informacji o rachunku te same informacje na temat wyznaczonych rachunków płatniczych i powiązanych transakcji płatniczych, które udostępniają użytkownikowi usług płatniczych, gdy ten bezpośrednio żąda dostępu do informacji o rachunku, **pod warunkiem, że informacje te nie zawierają szczególnie chronionych danych dotyczących płatności**[760]. Te dane są definiowane również przez uUP (art. 2 pkt 26c), gdzie szczególnie chronione dane dotyczące płatności to dane, w tym indywidualne dane uwierzytelniające (jak login czy hasło), które mogą być wykorzystywane do dokonywania oszustw (z wyjątkiem imienia i nazwiska lub nazwy właściciela rachunku i numeru rachunku). Nie wyklucza to oczywiście możliwości pozyskania tych danych na innej podstawie, jak np. na bazie zgody udzielonej zgodnie z Rozporządzeniem 2016/679[761], jednakże stanowi to i tak istotne ograniczenie. Tym bardziej, że katalog tych danych jest dość szeroki i może obejmować dane potencjalnie istotne z punktu widzenia realizacji samej usługi AIS. Z drugiej strony wydaje się, że założeniem prawodawcy unijnego było tutaj zmininalizowanie ryzyka potencjalnych oszustw oraz uszczerbku dla osób trzecich, np. *silent parties* (odbiorców transakcji płatniczych), przy jednoczesnym zapewnieniu pewnej efektywności usługi dostępu do informacji o rachunku.

Niemniej jednak, postulowanym rozwiązaniem byłoby rozszerzenie tego katalogu o rachunki inne niż płatnicze lub wyraźne wskazanie, że dotyczy to także rachunków powiązanych, np. technicznych, które są funkcjonalnie związane z rachunkiem płatniczym w stosunku, do którego realizowana jest usługa. Zmiany

---

758 Wyrok Trybunału z dnia z dnia 4 października 2018 r., C-191/17.

759 S. McInnes, K. Berg, *Some key topics under PSD2: open banking, strong customer authentication, and the platform/commercial agent exemption*, Tijdschrift voor INTERNETRECHT Nr. 3/4 juli 2019, s. 112.

760 Również European Banking Federation, *Guidance for implementation of the revised Payment Services Directive PSD2 Guidance*, 20 December 2019, s. 27, https://www.ebf.eu/wp-content/uploads/2020/01/EBF-PSD2-Guidance-Final-v.120.pdf : dostęp: 1.02.2022 r.

761 Więcej w wytycznych EDPB, Wytyczne 6/2020 w sprawie wzajemnych zależności między drugą dyrektywą w sprawie usług płatniczych a RODO, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_pl: dostęp: 1.02.2022 r.

powinny objąć także przepisy o ochronie danych osobowych, jakkolwiek może to być uwzględnione również w projekcie nowelizującym dyrektywę PSD2. W tym kontekście zasadnym wydaje się jasne określenie wymogów względem m.in. cichych stron, których dane mogą być przetwarzane w związku z realizacją usługi AIS. Autor ma jednocześnie świadomość, że zagadnienie to wymaga znacznie szerszego ujęcia, które jest związane także z samą definicją rachunku płatniczego i brakiem jednolitych definicji pozostałych rachunków funkcjonujących w obrocie gospodarczym. Jest to jednak niezwykle istotna kwestia z punktu widzenia całego sektora finansowego.

2.4. Brak standaryzacji API oraz problemy związane z udostępnianiem interfejsów

Jednym z wyzwań, które postawił przed bankami pakiet PSD2 jest kwestia (nie) dostępności interfejsów dostępowych dla TPP. Art. 32 ust. 1 Rozporządzenia 2018/389 wskazuje, że dostawcy prowadzący rachunek, o ile wprowadzili specjalny interfejs, muszą zapewnić temu interfejsowi dostępność i efektywność – w tym w zakresie wsparcia – na poziomie tożsamym z tym dla interfejsów udostępnianych użytkownikom usług płatniczych w celu uzyskania bezpośredniego dostępu do rachunku. Podmioty zobowiązane muszą monitorować tą efektywność i zapewnić nieustannie najwyższy poziom, a także nie stwarzać przeszkód w zakresie realizacji usług AIS oraz PIS (art. 32 ust. 3).

W praktyce jednak problematyka stwarzania przeszkód stanowi swoistą oś sporu pomiędzy bankowymi dostawcami rachunków a częścią niebankowych TPP. Europejski Urząd Nadzoru Bankowego poza opinią w tym przedmiocie[762], regularnie publikuje wyjaśnienia w tym zakresie[763]. Jednym z podnoszonych zarzutów jest brak zakładanego poziomu efektywności po stronie interfejsów, co powoduje, że realizacja usług dostarczanych użytkownikom przez TPP również nie jest na poziomie zapewniającym zadowolenie klientów. Z jednej strony może być to skutkiem niewłaściwego doboru zachęt (czy ich braku) do dołożenia wysokiego poziomu staranności w zakresie tych interfejsów (o czym mowa w podrozdziale 2.1), jak również obaw samych dostawców usługi prowadzenia rachunku o konkurencję i/lub bezpieczeństwo danych.

Podmioty te nie realizują także zawsze obowiązków związanych ze środkami awaryjnymi, o których mowa w art. 33 Rozporządzenia 2018/389, które mają „zastępować" specjalne interfejsy dostępowe, gdy nie działają one w sposób

762 EBA, Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC, EBA/OP/2020/10, 4 June 2020, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/884569/EBA%20Opinion%20on%20obstacles%20under%20Art.%2032%283%29%20RTS%20on%20SCA%26CSC.pdf : dostęp: 2.02.2022 r.

763 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2 : dostęp: 2.02.2022 r.

poprawny. W efekcie, TPP mogą być pozbawione możliwości realizacji usługi dla swoich klientów.

Rozwiązanie tej kwestii nie jest zadaniem łatwym, bowiem same przepisy, jak i wyjaśnienia w tym zakresie, są raczej przejrzyste, a problemem jest brak właściwego ich stosowania przez zobowiązane podmioty. W takim przypadku wydaje się, że pożądanym kierunkiem zmian byłoby wprowadzenie specyficznych sankcji za brak zgodności, jak również zobowiązane organów nadzorczych do dokonywania regularnej inspekcji poziomów efektywności. Te kwestie częściowo są już adresowane na poziomie obowiązujących przepisów, bowiem zgodność z pakietem PSD2 jest przykładowo elementem Badania i Oceny Nadzorczej przeprowadzanego przez Urząd Komisji Nadzoru Finansowego[764], a ewentualne braki mogą skutkować zastosowaniem przez Urząd narzędzi dyscyplinujących, do których KNF jest uprawniona na podstawie m.in. art. 138. Efektywność tych rozwiązań jest jednak co najmniej wątpliwa, na co wskazuje chociażby wezwania Europejskiego Urzędu Nadzoru Bankowego do bardziej zdecydowanych działań po stronie organów nadzorczych w kontekście zapewnienia zgodności API z odpowiednimi wymogami, o czym była już mowa w niniejszym opracowaniu.

Warto tutaj jednocześnie zwrócić uwagę, że także w wymiarze transgranicznym pakiet PSD2 nie wypełnił wszystkich luk, które mogłyby przybliżyć do pełniejszej realizacji koncepcji otwartej bankowości. Bank Rozrachunków Międzynarodowych zwrócił uwagę w jednym z raportów, że w przestrzeni finansowej funkcjonuje wiele standardów API[765], co powoduje, że możliwość szybkiej integracji oraz wejścia na wiele rynków jednocześnie jest znacznie ograniczona. W Polsce wypracowany został standard PolishAPI[766], którego autorami jest organizacja branżowa – Związek Banków Polskich – wraz ze swoimi ekspertami. Pomimo szerszej adopcji przez sektor bankowy, nie udało się jednak w pełni wdrożyć go jednolicie, jak również w niewielkim stopniu sektor bankowy wdrożył rozwiązania wykraczające poza regulacyjne minimum.

Rozwiązaniem tej kwestii może być zobowiązanie Komisji Europejskiej oraz Europejskiego Urzędu Nadzoru Bankowego do opracowania stosownych standardów technicznych, a następnie powszechnie obowiązującego standardu wdrożenia z jednoczesnym zobowiązaniem podmiotów do ich stosowania. Pozwoliłoby to na szybszą integrację w aspekcie transgranicznym, jak i krajowym, co może przyczynić się do rozwoju otwartej bankowości. Taki postulat należy „podtrzymać" również w kontekście otwartych finansów.

764 https://www.knf.gov.pl/knf/pl/komponenty/img/Metodyka_BION_bankow_2021_73447.pdf : dostęp: 2.02.2022 r.

765 BIS, *Report on open banking and application programming interfaces*, November 2019, https://www.bis.org/bcbs/publ/d486.pdf : dostęp: 2.02.2022 r.

766 https://polishapi.org/#docs : dostęp: 2.02.2022 r.

3. Pomiędzy otwartą bankowością a otwartymi (zdecentralizowanymi) finansami – konkluzje

Obszar finansów ulega nieustannym zmianom, które mają wpływ m.in. na włączenie finansowe[767], co jest skutkiem m.in. postępującej cyfryzacji[768]. Rozwijają się nie tylko finanse tradycyjne, utożsamiane zazwyczaj z bankowością, ale także finanse zdecentralizowane (*decentralized finance* – DeFi)[769] oparte o technologię rozproszonego rejestru (DLT) oraz łańcuch bloków (*blockchain)*, które pozornie wydają się realizować odmienne cele. Rozwój technologii łańcucha bloków spowodował, że rozwinęły się alternatywne finanse w postaci tzw. kryptoaktywów, w szczególności kryptowalut, które mają zastępować prawne środki płatnicze. Jednocześnie coraz więcej dyskutuje się nad możliwością wprowadzenia tzw. CBDC (*Central Bank Digital Currency*), czyli walut cyfrowych banków centralnych[770]. Jednocześnie Unia Europejska, zgodnie z deklaracją zawartą we wspomnianej już *Strategii dla cyfrowych finansów*, zamierza urzeczywistnić koncepcję otwartych finansów, choć jej ostateczny kształt nie jest jeszcze przesądzony. Tematyka jakkolwiek niezwykle interesująca, pozostaje poza zakresem opracowania.

Sposób, w jaki dzisiaj wielu klientów wykorzystuje usługi i produkty finansowe różni się znacznie od tego, jak wyglądało to 20 czy nawet 10 lat temu. Powszechne wykorzystanie tzw. Internet of Things (IoT), czyli internetu rzeczy oraz rozpowszechnienie się internetu o wysokiej przepustowości, prowadzi do postępującego gromadzenia danych o człowieku, co może być wykorzystywane również w bankowości. Równie intensywnie rozwija się również obszar szeroko rozumianej sztucznej inteligencji[771] (czy bardziej precyzyjnie analityki danych), która ma potencjał m.in. w obszarze zarządzania finansami osobistymi[772], w tym zarządzaniu budżetem.

---

767 P. K. Ozili, *Impact of digital finance on financial inclusion and stability*, Borsa Istanbul Review 18-4 (2018), March 2018.

768 Więcej na temat wpływu transformacji cyfrowej na obszar finansów (w:) E. S. Prasad, *The Future of Money. How Digital Revolution Is Transforming Currencies and Finance*, Cambridge 2021.

769 J. Chen, C. Bellavitis, B*lockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models*, s. 5, https://www.researchgate.net/profile/Yan-Chen--30/publication/337111343_Blockchain_Disruption_and_Decentralized_Finance_-The_Rise_of_Decentralized_Business_Models/links/6078884c907dcf667ba12209/Blockchain-Disruption-and-Decentralized-Finance-The-Rise-of-Decentralized--Business-Models.pdf : dostęp: 2.02.2022 r.

770 Tematyka istotnie wykracza poza ramy niniejszego opracowania. Więcej na temat CBDC (w:) R. Auer, J. Frost, L. Gambacorta, C. Monnet, T. Rice, H. Song Shin, *Central bank digital currencies: motives, economic implications and the research frontier*, BIS Working Paper No 976, https://www.bis.org/publ/work976.pdf : dostęp: 2.02.2022 r.

771 Więcej na temat definicji sztucznej inteligencji (w:) M. Nowakowski, *Ostatnie zmiany w ramach prawnych dla sztucznej inteligencji w Unii Europejskiej – krytyczna analiza*, Prawo Nowych Technologii nr 2/2021, s. 23.

772 M. Nowakowski, K. Waliszewski, *Artificial Intelligence and Algorithms Assisting Personal Finance. A Legal and Economic Perspective*, Przegląd Ustawodawstwa Gospodarczego 08/2021, s. 2-10.

Aby jednak nowe usługi finansowe mogły rozwijać się w sposób efektywny i z korzyścią dla wszystkich zainteresowanych konieczne jest stworzenie odpowiednich ram prawnych i regulacyjnych[773], które obok edukacji klientów oraz zmian o charakterze infrastrukturalnym oraz organizacyjnym, pozwolą na swobodniejsze wykorzystywanie danych (oczywiście za zgodą użytkowników) przy zachowaniu wysokiego poziomu bezpieczeństwa tych usług.

Prawdopodobnym, choć nie jedynym scenariuszem dla przyszłości otwartej bankowości jest jej ewolucja w kierunku otwartych finansów. Może to nastąpić poprzez zmianę dyrektywy PSD2, jak również wydanie zupełnie nowego aktu prawnego – być może rozporządzenia o powszechnym charakterze. Niezależnie od wyboru prawodawcy, problemy natury prawnej i regulacyjnej wskazane w niniejszym opracowaniu pozostaną aktualne i będą wymagały „rozstrzygnięcia". Dziś nie ma już wątpliwości, że finanse będą musiały ewoluować za sprawą nie tylko zmieniającego się otoczenia i postępującej cyfryzacji, ale też „innych" oczekiwań samych klientów. Masowy produkt przestaje być atrakcyjny, a konkurencja, w tym niebankowych fintechów, skłania do równie ewolucyjnych zmian. Powoduje to, że finanse stają się bardziej spersonalizowane i odpowiadające na potrzeby klienta. Do tego potrzeba jednak czegoś więcej niż z góry narzuconych obowiązków bez „wyrównania" ich odpowiednimi zachętami o zróżnicowanym charakterze.

773 P. Sironi, *Banks and Fintech...*, *op.cit.*, s. 49.