Dariusz Gradzi

FinTech/RegTech. Ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu wynikające z nowych technologii w obszarze płatności elektronicznych

W pierwszym kwartale 2019 r. odnotowano ponad 1,2 mld transakcji kartami debetowymi i ponad 100 mln kartami kredytowymi[1]. W drugim kwartale 2019 r. całkowita liczba transakcji bezgotówkowych wyniosła 1,43 mld, a ich wartość blisko 93 mld zł[2]. Badania pokazują, że najpopularniejszymi instrumentami płatniczymi są: karta płatnicza, rachunek bankowy z dostępem do konta przez internet i konto w serwisie PayPal[3]. W dobie nieodwracalnej digitalizacji sektora finansowego jest on szczególnie podatny na ryzyko związane z działalnością przestępczą, w tym terrorystyczną. Z tego powodu od wielu lat prowadzi się prace legislacyjne, których wynikiem są nowe regulacje. Mają one być odpowiedzią na zidentyfikowane zagrożenia. W praktyce jest jednak inaczej, ponieważ długość procesu legislacyjnego powoduje, że już w momencie wdrażania aktów prawnych nie są one dostosowane do zmieniającej się rzeczywistości.

Przeciwdziałanie praniu pieniędzy (ang. *anti money laundering*, AML) oraz finansowaniu terroryzmu (ang. *terrorist financing*, TF) w instytucjach finansowych jest normowane przez IV Dyrektywę AML (dalej: AMLD4)[4]. Integruje ona system AML/CTF (ang. *counter terrorist financing*, CTF – zwalczanie finansowania terroryzmu) z międzynarodowymi standardami zwalczania prania pieniędzy (ang. *money laundering*, ML) i finansowania terroryzmu, przyjętymi przez Financial Action Task Force (FATF)[5].

---

1 *Informacja o kartach płatniczych. I kwartał 2019 r.*, https://www.nbp.pl/systemplatniczy/karty/q_01_2019.pdf, s. 6, 15 [dostęp: 4 XII 2019].

2 *Informacja o kartach płatniczych. II kwartał 2019 r.*, https://www.nbp.pl/systemplatniczy/karty/q_02_2019.pdf, s. 16, 17 [dostęp: 4 XII 2019].

3 Zob. *Raport. „Płatności cyfrowe" 2019*, https://eizba.pl/wp-content/uploads/2019/11/PLATNOSCI_CYFROWE_2019.pdf?fbclid=IwAR1ol9GL6K85vybNy5iwjoctd4k7YPFuT1rki_OpLjTwSqw1DFpGNkBoXBk [dostęp: 2 XII 2019].

4 *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 25 maja 2015 w sprawie zapobiegania wykorzystywania systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE* (Dz. Urz. UE L 141 z 5 VI 2015 r., s. 73).

5 Znana także jako Groupe d'action financière (GAFI) – międzynarodowa Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy założona w 1989 r. Celem jej działania jest rozwój praktyk służących

Stosownie do tych standardów w AMLD4 przyjęto, jako zasadę, podejście oparte na ryzyku (ang. *risked-based approach*). Zakłada się w nim, że ryzyko ML/TF jest różne w poszczególnych krajach. Dlatego też państwa i ich organy nadzorcze (ang. *competent authorities*, CA) oraz uczestnicy obrotu prawnego muszą identyfikować ryzyko oraz na podstawie standardów zawartych w AMLD4 – nim zarządzać, tj. podejmować odpowiednie i adekwatne środki prawne. Dnia 30 maja 2018 r. została uchwalona V Dyrektywa AML (dalej: AMLD5), z datą implementowania przez państwa członkowskie UE do 10 stycznia 2020 r.[6] Europejska ocena ryzyka prania pieniędzy i finansowania terroryzmu[7] identyfikuje kilkadziesiąt produktów i usług potencjalnie narażonych na ryzyko ML/TF, w tym: bankowość prywatną, platformy crowdfundingowe (ang. *crowdfunding* – finansowanie społecznościowe[8]), waluty wirtualne, wartości majątkowe o właściwościach podobnych do gotówki, takie jak: złoto, diamenty.

Stosownie do regulacji ML/TF nie na każdy podmiot nałożono określone obowiązki prawne. Prawodawstwo AML/CTF dotyczy wyłącznie tzw. instytucji obowiązanych, za które – na gruncie polskiej ustawy o przeciwdziałaniu praniu pieniędzy[9] – uznaje się m.in. (w zakresie istotnym z punktu widzenia przedmiotu niniejszego opracowania):

- banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, instytucje finansowe mające siedzibę na terytorium RP;
- spółdzielcze kasy oszczędnościowo-kredytowe oraz Krajową Spółdzielczą Kasę Oszczędnościowo-Kredytową;
- krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego, oddziały unijnych instytucji płatniczych, oddziały unijnych i zagranicznych instytucji pieniądza elektronicznego, małe instytucje płatnicze, biura usług płatniczych oraz agentów rozliczeniowych;
- firmy inwestycyjne, banki powiernicze;
- zagraniczne osoby prawne prowadzące na terytorium Rzeczpospolitej Polskiej działalność maklerską;
- spółki prowadzące rynek regulowany;

---

zwalczaniu prania pieniędzy. Organizacja publikuje rekomendacje na ten temat, http://www.fatf-gafi.org/about/ [dostęp: 2 XII 2019].

6 *Dyrektywa PE i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE* (Dz. Urz. UE L 156 z 19 VI 2018 r., s. 43).

7 *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf [dostęp: 4 XII 2019].

8 Mechanizm crowdfundingu zakłada wynagrodzenie przez projektodawcę osób wpłacających pieniądze na rzecz projektu, w formie wcześniej ustalonej (przyp. red.).

9 *Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (t.j: DzU z 2019 poz. 1115, ze zm.).

- fundusze inwestycyjne, alternatywne spółki inwestycyjne, towarzystwa funduszy inwestycyjnych, zarządzający alternatywnymi spółkami inwestycyjnymi;
- zakłady ubezpieczeń;
- Krajowy Depozyt Papierów Wartościowych S.A.;
- przedsiębiorców prowadzących działalność kantorową;
- podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług w zakresie:
  - wymiany walut wirtualnych na środki płatnicze,
  - wymiany pomiędzy walutami wirtualnymi,
  - pośrednictwa w wymianie, o której mowa powyżej,
  - prowadzenia rachunków;
- przedsiębiorców niebędących innymi instytucjami obowiązanymi, świadczących usługi polegające na:
  - tworzeniu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej,
  - pełnieniu funkcji członka zarządu lub umożliwianiu innej osobie pełnienia tej funkcji, lub podobnej, w osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej,
  - zapewnieniu siedziby, adresu prowadzenia działalności lub adresu korespondencyjnego oraz innych pokrewnych usług osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej,
  - działaniu lub umożliwieniu innej osobie działania jako powiernik trustu, który powstał w drodze czynności prawnej,
  - działaniu lub umożliwieniu innej osobie działania jako wykonującej prawa z akcji lub udziałów na rzecz podmiotu innego niż spółka notowana na rynku regulowanym, podlegającym wymogom dotyczącym ujawniania informacji zgodnie z prawem UE lub podlegająca równoważnym standardom międzynarodowym;
- fundacje, w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- stowarzyszenia posiadające osobowość prawną, w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- przedsiębiorców, w zakresie, w jakim przyjmują lub dokonują płatności za towary w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- instytucje pożyczkowe.

Ryzyko ogólne dotyczące sektora usług finansowych

Wspólna opinia Europejskich Organów Nadzorczych[10] na temat ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, mającego wpływ na sektor finansowy Unii Europejskiej, dzieli ryzyko na: wspólne dla wszystkich sektorów usług finansowych oraz właściwe (specyficzne) tylko dla konkretnych sektorów[11]. Na podstawie powyższego dokumentu można wyróżnić następujące rodzaje ryzyka wspólnego dla wszystkich sektorów finansowych w Unii Europejskiej[12]:

- ryzyko wynikające z wycofania się Wielkiej Brytanii z UE (ang. *Brexit risk*),
- ryzyko związane z rozwojem nowych technologii (ang. *new technologies risk*),
- ryzyko związane z walutami wirtualnymi (ang. *virtual currencies risk*),
- ryzyko związane z rozbieżnością legislacyjną państw UE oraz odmiennymi praktykami nadzoru (ang. *legislative divergence risk and divergent supervisory practices risk*),
- ryzyko związane ze słabością kontroli wewnętrznej (ang. *weaknesses in internal controls risk*),
- ryzyko związane ze zjawiskiem de-riskingu (ang. *de-risking risk*)[13],
- ryzyko związane z finansowaniem terroryzmu (ang. *terrorist financing risk*).

Ryzyko wynikające z wycofania się Wielkiej Brytanii z UE[14]

Brexit niesie za sobą wyzwanie polegające na niepewności, czy organy nadzorcze państw członkowskich UE będą w stanie poradzić sobie ze sprawowaniem właściwego

[10] Ang. European Supervisory Authorities (ESA) – Europejskie Organy Nadzorcze. Na ESA składają się: European Securities and Markets Authority (ESMA) – europejski nadzór giełd i papierów wartościowych, European Insurance and Occupational Pensions Authority (EIOPA) – europejski nadzór ubezpieczeniowy i emerytalny oraz European Banking Authority (EBA) – europejski nadzór bankowy.

[11] *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector* (Wspólna opinia Europejskich Organów Nadzorczych w przedmiocie ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu wpływających na sektor finansowy UE, z 4 października 2019 r.), https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector [dostęp: 2 XII 2019].

[12] Tamże, s. 1.

[13] Ang. *de-risking* oznacza ograniczenie lub całkowite zaprzestanie przez instytucje obowiązane prowadzenia działalności, z którą są związane obowiązki wynikające z AMLD4, co w praktyce oznacza odmowę świadczenia usług dla podmiotów z obszarów o zwiększonym ryzyku ML i TF.

[14] W dniu 27 marca 2017 r. Wielka Brytania wyraziła intencję wycofania się z UE. Po wycofaniu się tego kraju z UE – przy braku stosowych umów – będzie on traktowany jako tzw. kraj trzeci (ang. *third country*). To oznacza, że nie będą się do niego stosowały regulacje prawne UE, a to z kolei będzie miało bezpośredni wpływ na sektor finansowy. Będzie on traktowany tak samo jak podmioty z krajów trzecich z siedzibą w Wielkiej Brytanii. Praktycznie oznacza to niestosowanie zasady jednego paszportu (ang. *single passport*), zasady jednolitej licencji (ang. *single licence*) i możliwości świadczenia regulowanych usług na terytorium całej UE, po uzyskaniu zezwolenia

i efektywnego nadzoru nad instytucjami finansowymi po ich relokacji z Wielkiej Brytanii na terytoria państw członkowskich UE. Przy braku umowy międzynarodowej, która unormuje m.in. stosunki prawne między Wielką Brytanią a Unią Europejską, ten kraj nie będzie już – w znaczeniu prawnym – traktowany jako państwo członkowskie UE.

To ryzyko jest szczególnie istotne, ponieważ od wielu lat Wielka Brytania jest zagłębiem firm fintechowych[15]. Sektor FinTech[16] w Wielkiej Brytanii wytwarza ponad 6,6 mld funtów zysku. Działa tam ponad 1,6 tys. tego rodzaju firm[17], obecne są m.in. takie spółki technologiczne, jak: Revolut, TransferWise, Monzo, Starling Bank, Oak North czy Funding Circle. W samej tzw. piaskownicy regulacyjnej[18] (ang. *regulatory sandbox*) funkcjonuje ok. 300 fintechów[19].

Do niedawna Europejski Urząd Nadzoru Bankowego (European Banking Authority, EBA)[20] miał swoją siedzibę w Londynie, jednak w związku z niepewnym statusem Wielkiej Brytanii jako członka UE siedziba została przeniesiona do Paryża (skutek wszczęcia procedury brexitu)[21].

Wycofanie się Wielkiej Brytanii z UE stwarza wiele sytuacji zakwalifikowanych jako ryzyko ML/TF. Zaliczono do nich[22]:

- sprawowanie nieefektywnego nadzoru nowych podmiotów,

w jednym kraju członkowskim.

15 https://biznes.wprost.pl/technologie/fintech/10013258/brexit-czy-wielka-brytania-straci-pozycje-lidera-fintech.html [dostęp: 2 XII 2019].
Fintechy – firmy finansowe działające wyłącznie w sieci (przyp. red.).

16 Ang. *FinTech* oznacza zastosowanie innowacyjnych rozwiązań technologicznych dotyczących sektora finansowego, skutkujące powstaniem nowych modeli biznesowych. Zob. *Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention* (raport Financial Stability Board (FSB) w sprawie implikacji FinTechu dla stabilności finansowej), https://www.fsb.org/wp-content/uploads/R270617.pdf, s. 33 [dostęp: 2 XII 2019].

17 https://www.money.pl/gospodarka/great-fintech-czyli-jak-to-sie-robi-w-wielkiej-brytanii-6440365075797633a.html [dostęp: 2 XII 2019].

18 Jest to powszechnie stosowany przez organy nadzorcze środek mający na celu umożliwienie spółkom technologicznym testowanie nowych produktów i usług finansowych bez konieczności ubiegania się i uzyskania skomplikowanych, czasochłonnych i kosztochłonnych licencji od tych organów, https://www.cashless.pl/cashlesspedia/piaskownica-regulacyjna [dostęp: 2 XII 2019]; https://www.knf.gov.pl/en/MARKET/Fintech/Regulatory_Sandbox [dostęp: 2 XII 2019].

19 Zob. raport *UK FinTech. State of the Nation*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf [dostęp: 2 XII 2019].

20 Urząd UE sprawujący nadzór nad systemem bankowym Unii. EBA został powołany 1 I 2011 r. na podstawie *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE* (Dz. Urz. UE L 331 z 15 XII 2010 r., s. 12).

21 https://www.consilium.europa.eu/en/policies/relocation-london-agencies-brexit/ [dostęp: 2 XII 2019].

22 *Joint Opinion of the European Supervisory Authorities*…, s. 10 [dostęp: 2 XII 2019].

- przeniesienie się podmiotów z Wielkiej Brytanii do innych państw członkowskich i konieczność dostosowania się przez te podmioty do nowych regulacji[23] oraz procedur *compliance*[24] (migracja regulacyjna),
- konieczność oceny wielu nowych podmiotów, ich modeli biznesowych, struktury własnościowej, organizacji kontroli wewnętrznej oraz ich monitoringu przez nowe organy nadzorcze,
- prowadzenie przez relokowane podmioty dalszej działalności w Wielkiej Brytanii, mających w państwach członkowskich UE wyłącznie formalne siedziby bez żadnych struktur (tzw. *shell companies* – spółki fasadowe),
- dostosowywanie się instytucji finansowych do procedury AML/CTF, gdyż po brexicie Wielka Brytania będzie tzw. państwem trzecim w rozumieniu AMLD4.

W przypadku wycofania się Wielkiej Brytanii z UE bez ratyfikowanej umowy lub przy braku porozumienia pomiędzy organami nadzorczymi Wielkiej Brytanii i UE, równoważnego takiej umowie, organy nadzorcze UE będą mogły, w ograniczonym zakresie, wymieniać informacje dotyczące przeciwdziałania ML/TF. Jeśli do brexitu dojdzie na podstawie umowy, wymiana informacji (która jest newralgiczna przy płatnościach elektronicznych, ponieważ bardzo często występują w nich elementy transgraniczne) będzie zależała od przyjętych warunków. W tej sprawie zawarto już tzw. *Memorandum of Understanding* (MoU)[25] pomiędzy europejskimi organami nadzoru a Financial Conduct Authority (FCA)[26].

Ryzyko związane z rozwojem nowych technologii[27]

Tego rodzaju ryzyko jest związane z nowymi dziedzinami FinTech oraz RegTech[28]. Przykładowymi rozwiązaniami fintechowymi są bezpieczne aplikacje mobilne[29]

---

[23] AMLD4 przewiduje pewne minimalne, wspólne standardy, a państwa członkowskie mają możliwość podwyższenia tych standardów przy implementacji AMLD.

[24] Ang. *compliance* jest rozumiane jako zapewnienie zgodności działań podmiotu z przepisami prawa oraz ich monitorowanie, https://www.rewi.europa-uni.de/pl/lehrstuhl/pr/poloerecht/projekte/Compliance/index.html [dostęp: 2 XII 2019].

[25] Memorandum określa zasady postępowania w przyszłości i wyraża wolę przyjęcia określonych zobowiązań, https://pressto.amu.edu.pl/index.php/cl/article/viewFile/6437/6458 [dostęp: 2 XII 2019]

[26] Odpowiednik polskiej Komisji Nadzoru Finansowego w Wielkiej Brytanii, https://www.fca.org.uk [dostęp: 2 XII 2019].

[27] *Joint Opinion of the European Supervisory Authorities*…, s. 12 [dostęp: 2 XII 2019].

[28] Ang. *RegTech* to zastosowanie nowych technologii służących wsparciu wymogów regulacyjnych i ich stosowaniu – definicja opracowana przez Międzynarodowy Instytut Finansów (ang. Institute of International Finance). Zob. https://www.iif.com/Innovation/Regtech [dostęp: 2 XII 2019]. Zob. też: *Financial Stability Implications from FinTech*…, s. 34 [dostęp: 2 XII 2019]. Trzeci termin (oprócz RegTech i FinTech) – ang. *InsureTech* – odnosi się do zastosowania nowoczesnych technologii w rozwiązaniach, które skutkują zwiększeniem funkcjonalności sektora ubezpieczeniowego.

[29] Aplikacje płatnicze do integracji z urządzeniami mobilnymi (np. telefon, iPad).

dla banków oraz usługi online (pożyczki) lub *factoring* online, w których cała procedura (np. udzielania kredytu) oraz ocena zdolności kredytowej (płatniczej) klienta odbywa się elektronicznie i zdalnie (ang. *remotely*), a podmioty oferujące te usługi korzystają m.in. z baz danych biur informacji gospodarczej, portali społecznościowych typu Facebook, LinkedIn lub Instagram.

Najważniejszymi podmiotami fintechowymi, które mają siedzibę w Polsce, są: PayU, Blue Media, Polish Payment Standard – Polski Standard Płatności (BLIK), Currency One, Finanteq, VoicePIN, ZenCard. Wśród zagranicznych można wyróżnić: Revolut[30] oraz N26[31].

Przykładami rozwiązań fintechowych z segmentu płatniczego są: system płatności BLIK[32], systemy płatności na urządzeniach mobilnych[33]: Google Pay, Apple Pay, Samsung Pay, a także płatności zbliżeniowe, niezwiązane lub związane z powyższymi systemami.

Z kolei narzędzia RegTech umożliwiają podmiotom szybsze, tańsze i łatwiejsze gromadzenie oraz analizowanie danych, do których weryfikacji są one zobowiązane[34]. Ma to szczególne znaczenie z punktu widzenia AML/TF (zwiększenie transparentności operacji finansowych). Przykładem może być automatyczna weryfikacja listy osób zajmujących eksponowane stanowiska polityczne (ang. *politically exposed person*, PEP), czyli – zgodnie z AMLD4 – m.in.: prezydentów, premierów, posłów, ministrów oraz członków ich rodzin. Jednym z rozwiązań RegTech jest interfejs programowania aplikacji (ang. *application programming interface*, API)[35] zaprojektowany dla konkretnej instytucji finansowej. To działanie wynika ze spełniania potrzeb danej instytucji lub dostarczania jej danych gospodarczych z wielu źródeł i takie ich zintegrowanie, aby ta instytucja finansowa, np. bank, otrzymała w jednym systemie wszystkie wymagane informacje[36].

Rozwój technologii otwiera nowe możliwości dla dostawców FinTech i RegTech, jednak niesie zagrożenia związane z ML/TF. Na podstawie wspomnianej już wspólnej

---

[30] https://www.revolut.com/pl-PL [dostęp: 2 XII 2019].

[31] https://n26.com/en-eu [dostęp: 2 XII 2019].

[32] https://blikmobile.pl [dostęp: 2 XII 2019].

[33] Są to płatności dokonywane przy użyciu mobilnego urządzenia wyposażonego w system operacyjny, z multimedialnym interfejsem z wykorzystaniem technologii radiowej, sieci telekomunikacyjnych bezprzewodowych (GSM, GPRS, UMTS, Wi-Fi, NFC, RFiD, Bluetooth), https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf [dostęp: 4 X 2017].

[34] http://fintechpoland.com/pl/projects/raport-regtech-znaczenie-innowacji-regulacyjnych-dla-sektora-finansowego-i-panstwa/ [dostęp: 2 XII 2019]; https://medium.com/blog-transparent-data/co-to-jest-regtech-i-jak-ma-się-do-fintech-f27bab5a3a55 [dostęp: 2 XII 2019].

[35] Interfejs programowania aplikacji; zestaw reguł opisujący, w jaki sposób programy komputerowe się ze sobą komunikują.

[36] Np. system Transparent Data, https://transparentdata.pl [dostęp: 2 XII 2019].

opinii Europejskich Organów Nadzorczych można zidentyfikować następujące rodzaje ryzyka wynikające ze stosowania FinTech[37]:

- świadczenie usług w postaci nieregulowanych produktów finansowych, które nie wchodzą w zakres prawodawstwa AML/CTF,
- poprawność informacji gromadzonych podczas procesu oceny klienta (ang. *customer due diligence*, CDD),
- niezrozumienie przez dostawców innowacyjnych technologii FinTech wymagań AML/CTF oraz pozostałych regulacji,
- różnice w kulturze *compliance*[38] pomiędzy nadzorowanymi podmiotami,
- powstawanie nowych technologii służących do zdalnego nawiązywania relacji z klientem (tzw. *onboarding*), bez zachowania środków bezpieczeństwa w zakresie zwalczania cyberprzestępczości oraz kradzieży tożsamości,
- zbytnie poleganie przez instytucje finansowe (np. banki) na *outsourcingu*[39] z fintechami, bez przykładania należytego znaczenia do mechanizmów ich kontroli (zjawisko powszechne w Polsce).

Przy wprowadzaniu nowych technologii wspomagających RegTech może wystąpić ryzyko związane z[40]:

- bezkrytycznym poleganiem firm na rozwiązaniach technologicznych, które może prowadzić do ograniczenia zaangażowania się ludzi w monitorowanie transakcji;
- brakiem regulacji prawnych w zakresie RegTech;
- niezrozumieniem nowych technologii wykorzystywanych w procesie oceny klientów, co czyni wprowadzające je podmioty podatnymi na zagrożenia ML/TF;
- zbytnim poleganiem na podmiotach, którym przekazano możliwość korzystania z pewnych procesów (zasada czystych rąk), bez należytego wglądu w ich działalność i procedury, co w konsekwencji może prowadzić do:
  - trudności w ocenie danych klienta,
  - wątpliwości w zakresie wiarygodności danych (rekordów), spowodowanych niebezpiecznymi praktykami ich pozyskiwania i przechowywania przez dostawców RegTech;
- brakiem transparentności przy przeniesieniu odpowiedzialności pomiędzy dostawcami RegTech, szczególnie gdy procesy zostały im przekazane na podstawie umowy *outsourcingowej* i te podmioty nie są instytucjami obowiązanymi na podstawie AMLD4.

---

[37] *Wspólna Opinia Europejskich Organów Nadzorczych*…, s. 12 [dostęp: 2 XII 2019].

[38] Zapewnienie zgodności działalności z regulacjami prawnymi, normami bądź zaleceniami (przyp. red.).

[39] Skrót od ang. słów: *outside-resource-using*. *Outsourcing* polega na przekazywaniu zadań, funkcji, projektów i procesów do realizacji firmie zewnętrznej (przyp. red.).

[40] *Joint Opinion of the European Supervisory Authorities*…, s. 13 [dostęp: 2 XII 2019].

Wymienione sytuacje stwarzające zagrożenie zostały opisane w opinii Europejskich Organów Nadzorczych (European Supervisory Authorities, ESA) dotyczącej używania innowacyjnych rozwiązań odnoszących się do CDD[41].

Transakcje finansowe zostały w pełni zdigitalizowane, co dostawcy różnych usług muszą uwzględnić, zwłaszcza że te zmiany istotnie zwiększają ryzyko ML/TF. Analiza profilu klienta ma podstawowe znaczenie z punktu widzenia obowiązków AML w zakresie identyfikacji i weryfikacji klienta. Można wyróżnić następujące rodzaje innowacyjnych rozwiązań przy ocenie klienta[42]:

- rozwiązania weryfikacyjne *non-face-to-face*, na podstawie tradycyjnych dokumentów tożsamości (paszport, prawo jazdy) z wykorzystaniem urządzeń mobilnych (np. smartfonu),
- rozwiązania weryfikacyjne oparte na centralnych repozytoriach dokumentów identyfikacyjnych (tworzonych jako przedsięwzięcia wspólne dla wielu firm lub zlecane zewnętrznemu partnerowi),
- rozwiązania, których podstawą jest sztuczna inteligencja (ang. *artificial intelligence*, AI) przetwarzająca znaczną ilość informacji z różnych źródeł, w różnych językach. Dzięki tym systemom można przeanalizować np. historię transakcji, lokalizację GPS, portale społecznościowe, publikacje internetowe, rejestry beneficjentów rzeczywistych, osób zajmujących eksponowane stanowiska polityczne lub członków ich rodzin. Pozwalają one także na zdalne wykrycie fałszywych dokumentów identyfikacyjnych na podstawie cech tych dokumentów (znaki wodne, fotografie, linie wrażliwe na promienie UV, układ graficzny dokumentu).

Ryzyko związane z walutami wirtualnymi

Milton Friedman zauważył, że: (…) *Internet stanie się jedną z głównych sił redukujących rolę rządów. Jedyną rzeczą, której nam brakuje, ale która z całą pewnością wkrótce zostanie rozwinięta, jest prawdziwa e-gotówka – metoda, dzięki której można przekazać poprzez Internet środki pomiędzy podmiotami A i B, przy czym zarówno podmiot A nie zna B, jak i podmiot B nie zna A*[43].

W płatniczym systemie finansowym można wyróżnić[44] następujące modele obrotu walutami:

---

[41] Zob. *Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process* (*Opinia o korzystaniu z innowacyjnych rozwiązań w procesie oceny profilu klienta przez instytucje kredytowe i finansowe*), https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf [dostęp: 2 XII 2019].

[42] Tamże, s. 5.

[43] Cyt. za A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018, s. 7.

[44] Tamże, s. 19.

- scentralizowany: istnieje jeden podmiot odpowiadający za emisję i kontrolę obrotu określoną walutą. Transakcje są realizowane wyłącznie za pośrednictwem tego podmiotu, który prowadzi rejestr wszystkich transakcji,
- zdecentralizowany: podmiot centralny przekazuje podległym mu strukturom część kompetencji i zadań do wykonania,
- rozproszony: nie występuje hierarchizacja. Żadna z jednostek nie pozostaje wobec innej jednostki w relacji: nadrzędność–podrzędność. Nie ma również żadnej jednostki centralnej. Każdy uczestnik obrotu ma możliwość kontaktu z pozostałymi. Może on być również emitentem waluty, może uczestniczyć w kontroli i nadzorze obrotu oraz dysponować rejestrem wszystkich transakcji w systemie (będącym właściwym dla obrotu walutami wirtualnymi).

Na system płatniczy składa się określona grupa instytucji i procedur wykorzystywanych do zapewnienia sprawnego obiegu pieniądza na danym obszarze geograficznym[45].

W ramach systemu płatniczego należy wyróżnić cztery poziomy aktywności uczestników:

- poziom pierwszy – podmioty będące stronami dokonywanych transakcji płatniczych,
- poziom drugi – podmioty bezpośrednie obsługujące procesowanie transakcji pomiędzy uczestnikami poziomu pierwszego; są to dostawcy usług płatniczych, np. banki i instytucje płatnicze,
- poziom trzeci – podmioty uczestniczące w rozliczaniu transakcji pomiędzy uczestnikami poziomu drugiego (np. polska Krajowa Izba Rozliczeniowa),
- poziom czwarty – podmioty przechowujące środki pieniężne dostawców usług płatniczych lub papiery wartościowe (np. Narodowy Bank Polski oraz Krajowy Depozyt Papierów Wartościowych).

W systemie płatniczym należy wyróżnić[46]:

- system płatności wysokokwotowych;
- system płatności detalicznych (retailowych, ang. *retail* – handel detaliczny), na który składają się:
  - podsystem płatności kartowych,
  - podsystem płatności mobilnych,
  - podsystem płatności natychmiastowych;
- system rozrachunku papierów wartościowych.

Waluty wirtualne (ang. *virtual currencies*, VC) nie są regulowanymi produktami finansowymi w UE, co powoduje narażenie klientów na ryzyko, które często jest niemożliwe do przewidzenia, a ich katalog jest otwarty[47]. Z uwagi na brak regulacji

[45] Tamże, s. 79.

[46] Tamże.

[47] Zob. *EBA Opinion on 'virtual currencies'* (Opinia EBA o walutach wirtualnych, z 4 lutego 2014 r.), https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b-94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20

na szczeblu UE ochrona w tym zakresie powinna spoczywać na krajowych organach nadzorczych. Europejski Urząd Nadzoru Bankowego od lat publikuje raporty wskazujące na zagrożenia związane z obrotem walutami wirtualnymi[48].

Powszechnie przyjmuje się podział walut wirtualnych na[49]:

- żetony – akceptowane głównie przez członków wirtualnych społeczności, które są emitowane i kontrolowane przez jego twórców, np. autorów gier komputerowych (żetony: Facebook Credits, Amazon Coins, które są scentralizowanymi walutami wirtualnymi); w tym przypadku emitent jest instytucją kontrolującą sferę podażową (emisję) oraz autoryzuje i rozlicza transakcje,
- kryptowaluty.

Europejski Bank Centralny definiuje kryptowaluty jako: (…) *cyfrowo prezentowaną wartość, która nie została wyemitowana przez bank centralny, instytucję kredytową, jak i instytucję pieniądza elektronicznego, która w pewnych okolicznościach, może być wykorzystana jako alternatywa wobec pieniądza*[50].

Najbardziej znanym przykładem waluty wirtualnej jest bitcoin. Za jego twórcę uznaje się osobę (lub osoby) o pseudonimie Satoshi Nakamoto, w której zamyśle bitcoin miał pozwalać na realizowanie bezpośrednich i anonimowych transakcji w handlu elektronicznym[51]. Ten system miał być niezależny od tradycyjnych instytucji finansowych, a operacje finansowe miały się odbywać w całkowitej separacji od ogólnoświatowych systemów finansowych oraz centralnych systemów rozliczeniowych.

David Chaum jest postrzegany jako „ojciec pieniądza cyfrowego" i „ojciec anonimowości w Internecie"[52]. Przedstawił on scentralizowany system anonimowych płatności zwiększających bezpieczeństwo i prywatność użytkowników w stosunku do innych systemów istniejących w tym czasie. W 1982 r. opublikował pracę *Blind signatures for untraceable payments*, w której opisał naruszanie prywatności przez istniejące systemy rozliczeń[53]. Podstawą założeń Chauma była konieczność ograniczenia wiedzy pośrednika finansowego na temat czasu, wartości i przedmiotu płatności,

Currencies.pdf?retry=1 [dostęp: 2 XII 2019].

[48] http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf; https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD; https://www.eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf [dostęp: 2 XII 2019].

[49] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 15.

[50] Tamże, s. 25.

[51] Tamże, s. 34–37. Założenia bitcoina zostały przedstawione w pracy *Bitcoin: A Peer-to-Peer Electronic Cash System*, autorstwa anonimowego autora o pseudonimie Satoshi Nakamoto. Uważa się jednak, że pod tym pseudonimem kryją się korporacje technologiczne: SAmsung, TOSHIba, NAKAmichi, MOTOrola.

[52] Tamże, s. 30.

[53] Tamże.

a także możliwości analizy zbyt wielu metadanych (ang. *big data*[54]). Dla pośrednika finansowego zbędne – z punktu widzenia płatności – są dane dotyczące: lokalizacji osoby, jej stylu życia (m.in. informacje o podróżach, opłacanych hotelach, rachunkach z restauracji, drobnych wydatkach, żywności, lekach, prasie, wsparciu instytucji politycznych i religijnych). Chum opracował tzw. ślepy podpis (podpis cyfrowy, nowy rodzaj kryptografii). To rozwiązanie prowadziło do uzyskania tzw. asymetrycznej anonimowości, w której płatnik był nieznany, ale osoba przyjmująca płatność mogła zostać zidentyfikowana, jeżeli zaszła taka potrzeba. Wadą tego rozwiązania była podatność na tzw. *double-spending*, tj. możliwość podwójnego wydatkowania tych samych środków[55].

W rozwoju kryptowalut nie można pominąć także tzw. ruchu *cypherpunk*[56], dla którego zwolenników prywatność była podstawą nowoczesnego i cyfrowego społeczeństwa. Nie wierzono, że zostanie ona zapewniona przez rządy. Mogła zostać zachowana wyłącznie dzięki zastosowaniu narzędzi szyfrujących i zdecentralizowanemu systemowi komunikacji. Pod wpływem tego ruchu jeden z jego członków przedstawił w 1998 r. projekt anonimowej waluty cyfrowej *b-money*. Podstawą dobrze funkcjonującego społeczeństwa cyfrowego było istnienie sprawnie działającego środka wymiany (pieniądza) oraz efektywnych sposobów egzekwowania umów. Najważniejszym elementem ruchu *cypherpunk* był projekt zasad dokonywania transakcji płatniczych bez udziału pośredników. Założono w nim, że wszystkie transakcje będą zapisywane w rejestrze, którego kopię ma każdy z jego uczestników. Dzięki temu taki rejestr jest niemożliwy do sfałszowania[57]. Powyższe koncepcje doprowadziły do powstania w 2008 r. kryptowaluty bitcoin, która została uruchomiona w 2009 r.

Waluty wirtualne a pieniądz elektroniczny[58]

Waluty wirtualne są często błędnie utożsamiane z tzw. pieniądzem elektronicznym[59]. Różnica między nimi poza sferą regulacyjną sprowadza się do tego, że waluta

[54] Używanie zaawansowanych technik w celu analizowania dużych zasobów zdywersyfikowanych danych, które mogą nie być ustrukturyzowane i mogą pochodzić z różnych źródeł, https://www.ibm.com/analytics/hadoop/big-data-analytics [dostęp: 2 XII 2019].

[55] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 30–31.

[56] *Cypherpunks* – działacze propagujący powszechne stosowanie silnej kryptografii jako drogi do zmian społecznych i politycznych. Pierwotnie tworzyli oni nieformalną grupę komunikującą się za pośrednictwem list dyskusyjnych, która za cel stawiała siebie osiągnięcie prywatności i bezpieczeństwa przez aktywne wykorzystanie kryptografii, za: https://pl.wikipedia.org/wiki/Cypherpunk [dostęp: 17 II 2010] – przyp. red.

[57] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 32–33.

[58] Komisja Nadzoru Finansowego w piśmie do banków z 10 lipca 2015 r. dokonała analizy prawnej emisji pieniądza elektronicznego, https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [dostęp: 2 XII 2019].

[59] W rozumieniu *Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych* (t.j.: DzU z 2019 r.

wirtualna jest sztuczną jednostką rozliczeniową, podczas gdy jednostka rozliczeniowa pieniądza elektronicznego jest wyrażona w jednostce mającej status prawnego środka płatniczego. Waluty wirtualne natomiast nie muszą mieć związku z pieniądzem tradycyjnym (ang. *fiat currency*, FC), nie musi on też być ich podstawą.

Czynnikiem wyróżniającym kryptowaluty pod względem technologicznym jest dostępność kodu źródłowego oraz otwarte oprogramowanie (ang. *open source*)[60]. Za zakwalifikowaniem danego instrumentu do kryptowalut przemawia zastosowanie rozproszonego systemu transakcji oraz oparcie konstrukcji na kryptografii. Musi też istnieć globalna, publiczna oraz rozproszona baza danych obejmująca zrealizowane transakcje przy użyciu kryptowaluty.

Podstawą bitcoina było otwarte oprogramowanie, czyli ogólnie dostępny kod źródłowy, dzięki czemu wszyscy mogli go na bieżąco analizować i ulepszać. Bitcoin umożliwiał również procesowanie bezpośrednich transakcji pomiędzy użytkownikami Internetu, wykorzystując protokół komunikacyjny osoba do osoby (ang. *peer-to-peer*, także: *person-to-person*, P2P[61]). To oznacza brak konieczności funkcjonowania centralnego serwera (repozytorium informacji o transakcjach) oraz brak potrzeby korzystania z pośrednika transakcji[62]. Nie występuje zatem pośrednictwo tzw. zaufanej trzeciej strony.

Transakcje bitcoinami są zapisywane w blokach, które następnie łączą się w łańcuch bloków, tj. zapis zatwierdzonych transakcji (ang. *blockchain*[63]). Te zapisy składają się na publiczną księgę (ang. *public ledger*), bazę danych, przechowywaną przez wszystkie komputery użytkowników sieci bitcoin. Nowatorstwo tego systemu polega na utworzeniu łańcucha bloków funkcjonujących w ramach publicznego rozproszonego rejestru transakcji dokonywanych bitcoinami, w którym niemożliwe jest wycofanie transakcji. Jest to korzystne dla akceptantów płatności (np. sklepu przyjmującego płatność w kryptowalucie), ale może być ryzykowne dla płatnika[64].

W systemie bitcoin nie funkcjonuje żadna jednostka centralna ani organy nadzorcze. Struktura użytkowników systemu bitcoin składa się z dwóch poziomów: poziom

poz. 659, ze zm.) oraz *Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE* (Dz. Urz. UE L 267 z 10 X 2009 r., s. 7).

[60] Oprogramowanie, które zezwala na używanie ich kodu źródłowego, https://pl.wikipedia.org/wiki/Otwarte_oprogramowanie [dostęp: 2 XII 2019].

[61] Oznacza on równorzędność uczestników sieci, tj. każdy komputer podłączony do sieci może wysyłać i odbierać dane w sieci, co umożliwia pobieranie plików oraz ich udostępnienie komputerom podłączonym do tej sieci, https://poradnikprzedsiebiorcy.pl/-peer-to-peer-definicja-historia-powstania-i-wplyw-na-rozwoj-internetu-cz-1 [dostęp: 2 XII 2019].

[62] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 35.

[63] https://blockgeeks.com/guides/what-is-blockchain-technology/ [dostęp: 2 XII 2019]; https://pl.wikipedia.org/wiki/Blockchain [dostęp: 2 XII 2019].

[64] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 51–53.

pierwszy obejmuje użytkowników – akceptantów, drugi – podmioty wspomagające procesowanie transakcji, jak pośrednicy płatności oraz platformy obrotu kryptowalutami.

Wszystkie platformy obrotu kryptowalutami są na liście ostrzeżeń publicznych Komisji Nadzoru Finansowego[65]. Do czasu objęcia ich przepisami AMLD4 nie musiały one stosować żadnych środków AML/CTF (w tym identyfikować i weryfikować klienta). Niejednokrotnie prowadziło to do sytuacji, w której środki pochodzące z tzw. nieautoryzowanych transakcji płatniczych wskutek przywłaszczenia danych dostępowych do rachunku bankowego (tzw. credentiali, ang. *credential* – poświadczenie) były przez systemy płatności natychmiast transferowane na te platformy i następnie lokowane w bitcoiny. Dzięki takiemu zabiegowi w zasadzie nie jest możliwe ustalenie sprawców przywłaszczeń i pociągniecie ich do odpowiedzialności karnej, dlatego postępowania były umarzane na etapie postępowań przygotowawczych w sprawie.

Bitcoin – przetwarzanie transakcji i wymiar prawny

Jednym z większych problemów transakcji w systemie bitcoin jest jego przepustowość. Szacuje się ją na poziomie jednej transakcji na sekundę lub maksymalnie siedmiu transakcji na sekundę. Dla porównania, średnia liczba transakcji na sekundę w usłudze PayPal wynosi 100, w Visie – 2 tys., przy czym maksymalna wydajność tego systemu wynosi 56 tys. transakcji na sekundę. Wykonywanie jednej transakcji w systemie bitcoin trwa od kilkunastu minut do godziny. Zarzutem kierowanym pod adresem tego systemu jest jego duża energochłonność. Funkcjonowanie systemu wymaga bowiem nieustannego dostarczania energii do urządzeń, a zapotrzebowanie na energię wzrasta wraz z rozwojem sieci. Szacunki wskazują, że jedna transakcja w systemie bitcoin pochłania średnie dzienne zapotrzebowanie na energię elektryczną półtora gospodarstwa domowego w USA, a dzienne koszty energii zużywanej przez ten system sięgają 15 mln dolarów. System bitcoina cechuje także pseudoanonimowość, którą należy wiązać z publicznym udostępnieniem zapisu o zrealizowanych transakcjach. Umożliwia to śledzenie i analizowanie transakcji oznaczonych konkretnym adresem IP komputera. Istotnym mankamentem jest protokół kryptograficzny. Dotychczas nie został on złamany, jednak teoretycznie jest to możliwe. Taka sytuacja może wystąpić, gdy ktoś uzyska więcej niż 50 proc. mocy obliczeniowej systemu. Może to doprowadzić do zmiany aktualnego stanu równowagi blockchain[66] i wielokrotnego wydawania tych samych jednostek wartości[67].

Aktywa (prawa) kryptograficzne są definiowane[68] jako wartości oparte na kryptografii i technologii rozproszonych rejestrów (ang. *distributed ledger technology*, DLT),

[65] Lista jest dostępna pod linkiem https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne [dostęp: 2 XII 2019].

[66] Zob. szerzej: https://www.bbva.com/en/difference-dlt-blockchain/, https://101blockchains.com/blockchain-vs-distributed-ledger-technology/ [dostęp: 2 XII 2019].

[67] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 123–127.

[68] Zob. *EBA reports on crypto-assets* (Raport EBA o kryptoaktywach, z 9 stycznia 2019 r.),

której jednym z przykładów jest blockchain. DLT to rozproszona baza danych z rejestrami, które można replikować. Są one współdzielone i zsynchronizowane wśród użytkowników[69].

Technologia blockchain (rozumiana jako jeden z rodzajów DLT) jest używana przede wszystkim do transferu bitcoinów pomiędzy osobami, przy użyciu kluczy prywatnych (służących do kontroli własności jednostek bitcoin) i publicznych. Do rejestrowania transferu jednostek bitcoin jest wykorzystywana DLT. W przypadku wygenerowania transakcji jest ona rozpowszechniana w całej sieci DLT, co – przy użyciu klucza prywatnego – pozwala zweryfikować, czy zbywca jest właścicielem jednostek bitcoin. DLT umożliwia przechowywanie, aktualizowanie i weryfikowanie informacji w sposób zdecentralizowany[70].

Obrót walutami wirtualnymi jest narażony na ryzyko prania brudnych pieniędzy i finansowania terroryzmu, czemu można zaradzić, uznając podmioty prowadzące taką działalność gospodarczą za instytucje obowiązane[71]. Dotyczy to świadczenia usług w zakresie:

- wymiany walut wirtualnych na środki płatnicze,
- wymiany pomiędzy walutami wirtualnymi,
- pośrednictwa w wymianach, o których mowa powyżej,
- prowadzenia rachunków w formie elektronicznej jako zbioru danych identyfikacyjnych, zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany.

W dyrektywie AMLD5 za instytucje obowiązane uznano dostawców kont waluty wirtualnej[72] (ang. *included custodian wallet provider*). Wprowadzono tu także definicję legalną walut wirtualnych. Określono je jako cyfrowe wyznaczniki wartości, które nie są emitowane ani gwarantowane przez bank centralny lub organ publiczny i nie muszą być powiązane z walutą prawnie obowiązującą, a także nie mają prawnego statusu waluty lub pieniądza, ale są akceptowane przez osoby fizyczne lub prawne jako środek wymiany i mogą być przekazywane, przechowywane lub sprzedawane drogą elektroniczną. W Polsce pod pojęciem „waluty wirtualne" rozumie się cyfrowe odwzorowanie wartości, którymi nie są[73]:

- prawne środki płatnicze emitowane przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,

https://eba.europa.eu/eba-reports-on-crypto-assets [dostęp: 2 XII 2019].

69 https://pl.wikipedia.org/wiki/Technologia_rozproszonego_rejestru [dostęp: 2 XII 2019].

70 A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 51–53.

71 Art. 2 ust. 1 pkt 12 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

72 Art. 3 pkt 19 AMLD5. Przez dostawcę kont waluty wirtualnej rozumie się podmiot świadczący usługi polegające na przechowywaniu prywatnych danych uwierzytelniających w imieniu swoich klientów na potrzeby posiadania, przechowywania i przekazywania walut wirtualnych.

73 Art. 2 ust. 1 pkt 26 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

- międzynarodowe jednostki rozrachunkowe, ustanawiane przez organizację międzynarodową i akceptowane przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
- pieniądze elektroniczne, w rozumieniu ustawy o usługach płatniczych[74],
- instrumenty finansowe, w rozumieniu ustawy o obrocie instrumentami finansowymi[75],
- weksle lub czeki wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany.

Waluty wirtualne zalicza się do tzw. wartości majątkowych[76], do których należą także prawa majątkowe, inne mienie ruchome lub nieruchomości, środki płatnicze, instrumenty finansowe w rozumieniu ustawy o obrocie instrumentami finansowymi, inne papiery wartościowe oraz wartości dewizowe.

Europejski Urząd Nadzoru Bankowego oraz Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (European Securities and Markets Authority, ESMA[77]) opublikowały raport na temat zastosowania prawa UE do kryptoaktywów majątkowych (ang. *crypto-assets*)[78]. Na podstawie powyższego raportu można wymienić następujące zagrożenia związane z walutami wirtualnymi:

- brak wiedzy na temat funkcjonowania dostawców walut wirtualnych oraz ich produktów,
- rosnąca liczba transakcji online ze znikomą identyfikacją i weryfikacją klienta.

W 2018 r. FATF przyjął rekomendację (Rekomendacja 15[79]) mającą na celu włączenie do Rekomendacji definicji „*virtual assets*" i „*virtual assets service providers*". W konsekwencji w stosunku do tych aktywów i podmiotów obowiązuje obecnie prawodawstwo UE w zakresie przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu. Kryptoaktywa oznaczają:

- aktywa oparte na kryptografii i DLT lub zbliżonych technologiach,
- aktywa, które nie są używane i gwarantowane przez bank lub władze publiczne,
- aktywa, które mogą być wymieniane i stosowane w celach inwestycyjnych lub ułatwiających dostęp do dóbr i usług.

Przyjmuje się, że waluty wirtualne mogą spełniać prawne kryteria dla pieniądza elektronicznego i podlegać wszystkim wymogom regulacyjnym dotyczącym pieniądza tego rodzaju, w przypadku gdy:

---

[74] *Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych* (t.j.: DzU z 2019 r. poz. 659, ze zm.).

[75] *Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi* (t.j.: DzU z 2018 r. poz. 2286, ze zm.).

[76] Art. 2 ust. 2 pkt 27 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

[77] https://www.esma.europa.eu/about-esma/esma-in-short/whos-who [dostęp: 2 XII 2019].

[78] Zob. *Advice: initial coin offerings and crypto-assets*, ESMA50-157-1391, z 9 I 2019 r., https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf [dostęp: 2 XII 2019].

[79] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html [dostęp: 2 XII 2019].

- są przechowywane elektronicznie,
- mają wartość pieniężną,
- zawierają w sobie określone roszczenia do wydawcy walut wirtualnych,
- są wydawane w zamian za otrzymane środki,
- są wydawane w celu dokonywania płatności,
- są akceptowane przez inne podmioty, niebędące tylko wydawcą.

Waluty wirtualne są definiowane przez EBA jako[80]:

- mające wymiar cyfrowy swojej wartości (ang. *digital representation of value*), co nie wyłącza możliwości istnienia fizycznego odpowiednika,
- nieemitowane przez bank centralny lub inny organ władzy publicznej,
- niemające związku z tradycyjną walutą,
- akceptowalne przez osoby prawne i fizyczne jak środek płatniczy,
- te, które można przekazywać, przechowywać lub zbywać elektronicznie.

W *Opinii*... EBA zidentyfikowano około 70 szczegółowych rodzajów ryzyka związanych z walutami wirtualnymi, m.in.:[81]

- ryzyko dla użytkowników (ang. *risks to users*),
- ryzyko dla innych uczestników (ang. *risks to other market participants*),
- ryzyko dla integralności finansowej (ang. *risks to financial integrity*),
- ryzyko dla systemów płatności w walutach tradycyjnych (ang. *risks to payment systems in fiat currencies*),
- ryzyko dla regulatorów i organów nadzorczych (ang. *risks to regulators*).

Ryzyko związane z rozbieżnością legislacyjną państw UE oraz odmiennymi praktykami organów nadzorczych

To ryzyko wynika z zasady minimalnej harmonizacji[82] uwzględnionej w dyrektywach UE. Jest ono też zwiększane przez odmienną implementację[83] dyrektyw AMLD do prawnych porządków państw członkowskich.

Różnice w spójnym stosowaniu aktów prawnych dotyczących przeciwdziałania praniu pieniędzy dodatkowo są pogłębiane przez rozbieżne praktyki organów nadzorczych w państwach członkowskich w odniesieniu do tych samych zagadnień. Różnice w tych praktykach mogą wynikać z:

- innego podejścia opartego na ryzyku,
- odmiennego rozumienia ryzyka ML/TF przez organy nadzorcze,

---

[80] Zob. *EBA Opinion on 'virtual*…, s. 11; *EBA reports on crypto-assets*…

[81] Tamże, s. 5.

[82] Minimalna harmonizacja oznacza, że prawodawca unijny wyznacza wspólny i minimalny standard regulacji danego obszaru, https://www.eversheds-sutherland.com/documents/global/poland/articles_pdf/pl/2011-12-01_eps_prawo_konsumenckie_ue_dyrekywy_oparte_na_harmonizacji_minimalnej_akunkiel.pdf, s. 46 [dostęp: 2 XII 2019].

[83] Wprowadzenie dyrektywy UE do krajowego porządku prawnego.

- różnych środków zaangażowanych w nadzór ML/TF w poszczególnych państwach członkowskich.

Zagrożenia płynące z odmienności w zakresie legislacji powodują, że niektóre podmioty uzyskują zezwolenia w krajach podchodzących bardziej liberalnie do tego procederu, co wiąże się ze świadczeniem przez te podmioty usług w innych państwach członkowskich UE.

W pewnych krajach przepisy AML zostały w taki sposób implementowane, że organy nadzorcze nie mogą działać dopóty, dopóki nie znajdą dowodu działalności przestępczej. Z uwagi na obowiązującą zasadę jednolitego paszportu takie praktyki organów nadzorczych są szczególnym zagrożeniem, ponieważ jeżeli podmiot raz uzyska zezwolenia, może on swoją działalnością zagrażać innym rynkom państw członkowskich.

Na gruncie poprzednich dyrektyw AML nie było wprost wyartykułowanego obowiązku współpracy pomiędzy organami informacji finansowej poszczególnych państw w zakresie wymiany informacji. Z tego też powodu istniało ryzyko, że te organy mają tylko częściowy ogląd sytuacji ML/TF. Inaczej zostało to przedstawione w AMLD5. Te przepisy będą uzupełnione wytycznymi co do współpracy oraz wielostronnych umów o wymianie informacji.

Ryzyko wynikające z rozbieżnych praktyk nadzorczych[84]

Komitet Moneyval[85] i FATF od dłuższego czasu kwestionowały niektóre praktyki AML/CTF wybranych państw odnośnie ich adekwatności do występujących zagrożeń prania pieniędzy i finansowania terroryzmu. Europejski Urząd Nadzoru Bankowego sformułował przeciwko jednemu z nadzorców zarzuty dotyczące naruszenia prawa UE[86] w związku z niewywiązywaniem się z wymagań przeciwdziałania praniu pieniędzy.

Odmienne podejścia organów nadzoru do podmiotów nadzorowanych wynikają z:

- różnic w poziomach ryzyka,
- bezkrytycznego przyjmowania podejścia organów innych państw członkowskich w określonych sektorach do szacowanego ryzyka,
- różnic w wyszkoleniu personelu zwalczającego ML/FT.

---

[84] *Joint Opinion of the European Supervisory Authorities*…, s. 17 [dostęp: 2 XII 2019].

[85] Działający przy Radzie Europy komitet do oceny środków przeciwdziałających praniu pieniędzy i finansowaniu terroryzmu, https://www.coe.int/en/web/moneyval/ [dostęp: 2 XII 2019].
Pełna nazwa: Komitet Specjalny Ekspertów Rady Europy ds. Oceny Środków Przeciwdziałania Praniu Pieniędzy w Krajach Europy Środkowej i Wschodniej funkcjonujący w ramach Rady Europy, będący tzw. ciałem regionalnym FATF, za: https://www.kic.gov.pl/pl/documents/764034/1002265/20120911_MONEYVAL_inf.pdf [dostęp: 18 II 2020] – przyp. red.

[86] Rekomendacja dotyczyła maltańskiej jednostki analityki finansowej, https://www.eba.europa.eu/-/eba-issues-recommendation-to-the-maltese-financial-intelligence-analysis-unit-in-relation-to-its-supervision-of-pilatus-bank [dostęp: 2 XII 2019].

Ryzyko związane ze słabością kontroli wewnętrznej[87]

To ryzyko wynika ze słabej implementacji środków identyfikacji i weryfikacji klienta korzystającego z systemu bankowego. Jednym z głównych założeń AMLD4 było wprowadzenie przez instytucje obowiązane systemów kontroli wewnętrznej dopasowanych do ryzyka, na które jest narażony dany podmiot w związku ze swoją działalnością.

Jakkolwiek organy nadzorcze stoją na stanowisku, że w podmiotach nadzorowanych wprowadzono odpowiednie systemy kontroli wewnętrznej, szczególnie w zakresie rejestrowania transakcji, identyfikacji i weryfikacji klienta oraz raportowania transakcji podejrzanych, to dane otrzymywane przez Europejskie Organy Nadzorcze prowadzą do wniosku, że funkcjonowanie w praktyce tych polityk jest nieefektywne[88].

Kolejnym mankamentem są niewystarczające środki organizacyjne instytucji nadzorowanych w zakresie AML/CFT. Organy nadzorcze identyfikują najczęstsze naruszenia wymagań prawnych AML/CFT polegające na:

- niewystarczającej kontroli wynikającej z niewłaściwej identyfikacji i weryfikacji klienta, także beneficjentów rzeczywistych,
- nieadekwatnej do zagrożeń kontroli wewnętrznej, spowodowanej niewłaściwymi politykami i procedurami AML/CFT oraz nieprawidłową oceną ryzyka klienta.

Ryzyko wynikające ze zjawiska de-riskingu[89]

Przyczyną zjawiska deriskingu jest niewłaściwe podejście instytucji obowiązanych na podstawie ustawodawstwa AML/ CTF do zarządzania ryzykiem ML/TF, polegające na odmowie wchodzenia w relacje biznesowe z klientami ocenionymi jako stwarzającymi podwyższone ryzyko z punktu widzenia polityk ML/TF instytucji obowiązanych. Takie podejście prowadzi do „wypchnięcia" tych podmiotów do sfer, w których pozostają poza jakąkolwiek kontrolą. To z kolei powoduje, że sektor finansowy jest narażony na ryzyko ML/TF. Brak dostępu podmiotów wykluczonych do systemu finansowego prowadzi do dokonywania przez nie transakcji poza systemami kontroli AML/CFT. Schodzą one do nieformalnych kanałów płatniczych w celu zaspokojenia swoich potrzeb (głównie dokonując transakcji gotówkowych, co powoduje, że śledzenie tego rodzaju transakcji staje się niemożliwe)[90].

Europejskie Organy Nadzorcze stoją na stanowisku, że przy metodzie *risked-based approach* nie wymaga się od instytucji obowiązanych wypowiadania umów bądź kończenia relacji biznesowej tylko z powodu ustalenia wyższego ryzyka prania pieniędzy i finansowania terroryzmu. Takie podejście, zamiast zapobiegać tym zjawiskom, wzmagałoby to ryzyko.

---

[87] *Joint Opinion of the European Supervisory Authorities*…, s. 20 [dostęp: 2 XII 2019].

[88] Tamże, s. 20.

[89] Tamże, s. 25.

[90] Tamże.

Ryzyko finansowania terroryzmu[91]

Organy nadzorcze raportują, że największym problemem związanym z ryzykiem finansowania terroryzmu jest słabość systemu kontroli w zakresie monitoringu transakcji. Osoby finansujące terroryzm niekonieczne mogą chcieć ukryć swoją tożsamość, mogą również posługiwać się środkami z legalnych źródeł (np. finansowanie społecznościowe). Z tego powodu identyfikacja i weryfikacja klienta schodzą na plan dalszy, ustępując miejsca właściwemu monitorowaniu transakcji[92].

Walkę z finansowaniem terroryzmu utrudnia brak dostępu do istotnych informacji, często będących w posiadaniu organów ścigania, które pomogły na wczesnym etapie zidentyfikować zagrożenie. Dlatego tak ważne jest podjęcie współpracy organów ścigania z organami nadzorczymi, ponieważ każdy z tych podmiotów ma ogląd tej samej sytuacji z innej perspektywy.

Ryzyko specyficzne dotyczące sektora usług finansowych

Ryzyko specyficzne sektorowe zostanie zaprezentowane wspólnie dla instytucji: kredytowych[93], płatniczych, pieniądza elektronicznego – jako instytucji najbardziej podatnych na zagrożenia ML/TF. Można wyróżnić następujące podstawowe problemy w tym obszarze:

- ryzyko charakterystyczne dla danego sektora,
- jakość kontroli i najczęstsze naruszenia przepisów w sektorze finansowym, m.in.:
  - niewłaściwy poziom identyfikacji i weryfikacji klienta przez instytucje finansowe, ryzyko powiązane z modelami biznesowymi klientów,
  - monitorowanie współpracy, w tym monitorowanie transakcji,
  - ocena całościowego profilu ryzyka sektora.

Do symptomów wskazujących na podwyższone ryzyko ML/TF zaliczono następujące zachowania klienta:

- podejmowanie decyzji niezrozumiałych pod względem ekonomicznym, brak zainteresowania korzystniejszymi warunkami finansowymi produktu,
- wypłacanie dużych kwot z bankomatów,
- częste dokonywanie transakcji o podobnej wartości,
- brak orientacji w cechach produktu,
- sposób zachowania lub obecność osoby towarzyszącej wskazujące na to, że klient jest kontrolowany i nie podejmuje samodzielnie decyzji,

[91] Tamże, s. 24.

[92] Tamże.

[93] Art. 4 ust. 1 pkt 17 *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* (t.j.: DzU z 2019 r. poz. 2357).

- odmowa wykonania czynności związanych z jego identyfikacją i weryfikacją,
- rezygnacja z dokonania transakcji w przypadku, gdy dana instytucja okazuje zainteresowanie klientem,
- propozycja wręczenia korzyści majątkowej osobie dokonującej identyfikacji w zamian za nieprzeprowadzenie tej czynności lub wadliwe jej przeprowadzenie,
- posługiwanie się dokumentami wątpliwymi co do ich autentyczności.

Instytucje kredytowe oraz banki [94]

Instytucje kredytowe[95] (ang. *credit institutions*, CI) oraz banki są wykorzystywane przez klientów objętych ryzykiem ML/TF jako instytucje wejścia do systemu finansowego[96]. Jest to szczególnie widoczne w przypadku otwierania rachunków bankowych na podstawie przelewu weryfikacyjnego[97]. Komisja Nadzoru Finansowego uznała, że zawieranie umowy rachunku bankowego z wykorzystaniem przelewu weryfikacyjnego z innego rachunku płatniczego jako sposobu potwierdzania tożsamości klienta jest dopuszczalne, w przypadku gdy nie będzie możliwe kolejne zawarcie umowy rachunku płatniczego u innego dostawcy usług płatniczych, z wykorzystaniem przelewu z otwieranego rachunku dla potwierdzania tożsamości u tego dostawcy.

Również transakcje gotówkowe są czynnikiem powodującym rozwój zagrożenia ML/TF, zwłaszcza że większość instytucji kredytowych to instytucje retailowe, tj. konsumenckie i masowe. Występuje wówczas narażenie tych instytucji na transakcje transgraniczne, zwłaszcza tam, gdzie państwo członkowskie jest postrzegane jako centrum finansowe.

Na podstawie danych zawartych w wykresie 1 zamieszczonym na następnej stronie można zaobserwować roczny wzrost liczby naruszeń przepisów dotyczących zwalczania prania pieniędzy.

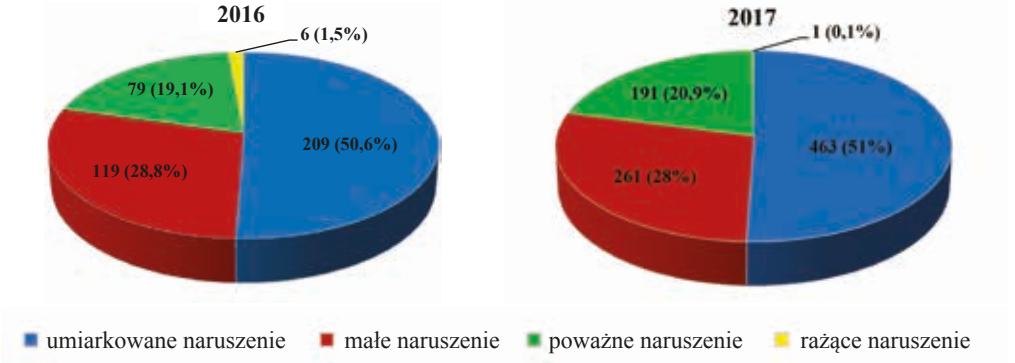
---

[94] *Joint Opinion of the European Supervisory Authorities*…, s. 30 i nast. [dostęp: 2 XII 2019].

[95] Art. 4 ust. 1 pkt 17 ustawy prawo bankowe.

[96] D. Chodziński, *Pranie pieniędzy jako jedna z form działania zorganizowanych grup przestępczych*, Legionowo 2012, s. 19, http://www.csp.edu.pl/download/6/16760/PraniepieniedzyjakojednazformdzialaniazorganizowanychgrupprzestepczychDChodzinsk.pdf [dostęp: 4 XII 2019].

[97] Zob. wytyczną nr 6 do *Rekomendacji KNF dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe*, z listopada 2015 r., https://zarabiajnabankach.pl/wp-content/uploads/2016/07/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf, s. 16 [dostęp: 2 XII 2019].



Wykres 1. Naruszenia przepisów dotyczących zwalczania prania pieniędzy.

Źródło: *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector* (Wspólna opinia Europejskich Organów Nadzorczych na temat ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu wpływającego na sektor finansowy UE, z 4 października 2019 r.), https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector, s. 34 [dostęp: 2 XII 2019].

Wydawcy pieniądza elektronicznego (ang. electronic money issuers, EMI)[98]

Poziom ryzyka związanego z wydawaniem pieniądza elektronicznego zależy przede wszystkim od: metod dostępu do produktów e-money (np. zdalny on-boarding klientów[99]), cech produktów e-money, stopnia, w jakim EMI korzystają z innych podmiotów do dystrybucji i umarzania e-money w ich imieniu.

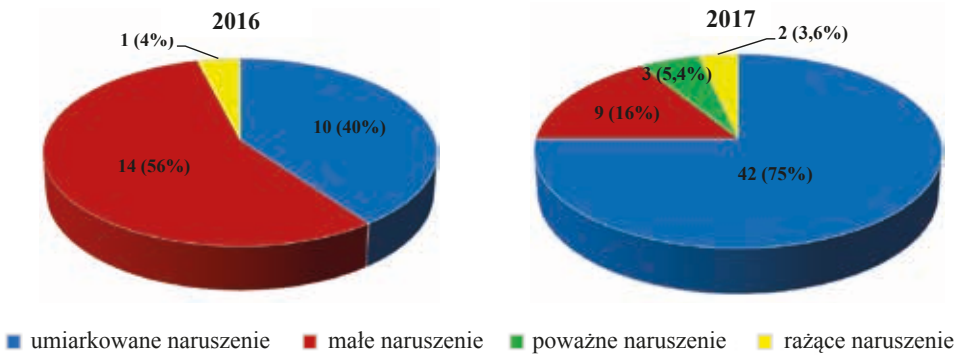
Im więcej wprowadza się restrykcji dotyczących użycia produktu e-money, tym mniejsza podatność na ML/TF. Wśród stosowanych restrykcji należy wymienić m.in.: limity płatności, brak możliwości dokonywania transakcji ATM (bankomatowych), akceptacja e-money możliwa w ograniczonej sieci akceptantów[100], brak transakcji osoba do osoby (P2P) oraz brak transakcji transgranicznych. Jednocześnie wymienione powyżej restrykcje sprawiają, że zastosowanie e-money jest ograniczone[101]. Do najczęstszych naruszeń w sektorze EMI zalicza się niewystarczające monitorowanie polityki i procedur, niska świadomości ML/TF, a także brak skuteczności raportowania transakcji podejrzanych (ang. *suspicious transaction reporting*, STR). W sektorze EMI obserwuje się wzrost liczby „naruszeń poważnych" oraz znaczny wzrost liczby „naruszeń umiarkowanych" (ang. *moderate breaches*), co zostało przedstawione na wykresie 2.

[98] *Joint Opinion of the European Supervisory Authorities*…, s. 46.

[99] To jest zdalne zawieranie umów z klientem.

[100] W rozumieniu art. 2 pkt 1b ustawy o usługach płatniczych.

[101] KNF do 2019 r. udzieliła tylko jednego zezwolenia na wydawanie pieniądza elektronicznego. Otrzymała je spółka Billon Solutions, https://businessinsider.com.pl/finanse/billon-solutions-licencja-e-money/xjb6be1, https://billongroup.com/pl/ [dostęp: 2 XII 2019].



Wykres 2. Naruszenia przepisów związanych z używaniem pieniądza elektronicznego.

Źródło: *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector* (Wspólna opinia Europejskich Organów Nadzorczych na temat ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu wpływającego na sektor finansowy UE, z 4 października 2019 r.), https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector, s. 50 [dostęp: 2 XII 2019].

Instytucje płatnicze (ang. payment institutions, PI)[102]

Ryzyko prania pieniędzy i finansowania terroryzmu w sektorze instytucji płatniczych[103] wiąże się głównie z rodzajem świadczonych usług oraz typem klienta. Największe ryzyko niosą za sobą przekazy pieniężne[104], zwłaszcza rozliczenia gotówkowe.

Podwyższony stopień wprowadzonych restrykcji ML/TF, dotyczący tego sektora, doprowadził do praktyk de-riskingu, stosowanych przez banki wobec dostawców usług przekazu pieniężnego działających w regionach o podwyższonym ryzyku ML/TF.

Przekazy pieniężne mają szczególne znaczenie w przypadku usług oferowanych klientom niemającym dostępu do regulowanych usług finansowych albo mającym ograniczony do nich dostęp. Wśród takich usług zaobserwowano używanie systemu hawala[105] do celów ML/TF przez dokonywanie niskokwotowych transferów pieniężnych[106].

[102] *Joint Opinion of the European Supervisory Authorities*…, s. 52.

[103] W rozumieniu art. 2 pkt 11 ustawy o usługach płatniczych.

[104] W rozumieniu art. 3 ust. 3 ustawy o usługach płatniczych.

[105] Pojmowany jako nieformalny transfer środków bez zaangażowania podmiotów autoryzowanych (jak banki). Zob. *System Hawala i finansowanie terroryzmu*, http://www.nowastrategia.org.pl/system-hawala-i-finansowanie-terroryzmu/ [dostęp: 2 XII 2019].

[106] Zob. *Krajowa Ocena Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu*, https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu, s. 125 [dostęp: 2 XII 2019].

Najczęstsze naruszenia w sektorze instytucji płatniczych

Organy nadzorcze obserwują, że polityka instytucji płatniczych w odniesieniu do identyfikacji i weryfikacji klienta, rejestru transakcji i STR jest dostosowana do obowiązujących przepisów. Problematyczna jest jednak efektywność zastosowanych praktyk. Obawy rodzi również niska świadomość instytucji płatniczych dotycząca zagrożeń ML/TF, która wynika z niewłaściwej oceny ryzyka klienta oraz jego działalności biznesowej (powodem może być m.in. konieczność szybkiego procesowania transakcji).

Podsumowanie

Analiza powyższych regulacji prawnych oraz stanowisk poszczególnych organów nadzorczych prowadzi do wniosku, że z uwagi na bardzo szybki postęp digitalizacji płatności elektronicznych te przepisy już w momencie wydania lub implementacji do krajowego systemu prawnego nie są adekwatne do zmieniającej się rzeczywistości. Pociąga to za sobą zwiększoną podatność systemu na ryzyko prania pieniędzy i finansowania terroryzmu.

Liczba wprowadzanych regulacji prawnych, zarówno w Unii Europejskiej, jak i w Polsce, oraz stopień ich skomplikowania pozwalają na wyciągnięcie wniosku, że ilekroć mamy do czynienia z innowacjami, to Amerykanie je wymyślają, Chińczycy kopiują, a Europejczycy regulują przepisami prawnymi. Dobitnie świadczy o tym to, że pomimo istniejącej od wielu lat możliwości wydawania pieniądza elektronicznego, pierwsze zezwolenie w tym zakresie zostało w Polsce udzielone dopiero w 2019 r.

Rynek płatności elektronicznych, a także organy nadzorcze stoją przed wyzwaniami związanymi z rozwojem FinTech oraz RegTech oraz śledzeniem trendów w obszarze walut wirtualnych. Instytucje finansowe i organy nadzorcze muszą współpracować ze sobą, m.in. przy wymianie informacji, oraz przeciwdziałać praktykom de-riskingu.

Bibliografia

Chodziński D., *Pranie pieniędzy jako jedna z form działania zorganizowanych grup przestępczych*, Legionowo 2012, Centrum Szkolenia Policji, http://www.csp.edu.pl/download/6/16760/PraniepieniedzyjakojednazformdzialaniazorganizowanychgrupprzestepczychDChodzinsk.pdf [dostęp: 4 XII 2019].

EBA Opinion on 'virtual currencies', https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 [dostęp: 2 XII 2019].

EBA reports on crypto-assets, https://eba.europa.eu/eba-reports-on-crypto-assets [dostęp: 2 XII 2019].

Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention, https://www.fsb.org/wp-content/uploads/R270617.pdf [dostęp: 2 XII 2019].

Informacja o kartach płatniczych. I kwartał 2019 r., Narodowy Bank Polski, https://www.nbp.pl/systemplatniczy/karty/q_01_2019.pdf [dostęp: 4 XII 2019].

Informacja o kartach płatniczych. II kwartał 2019 r., Narodowy Bank Polski, https://www.nbp.pl/systemplatniczy/karty/q_02_2019.pdf [dostęp: 4 XII 2019].

Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector [dostęp: 2 XII 2019].

Krajowa Ocena Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu, Ministerstwo Finansów, https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu [dostęp: 2 XII 2019].

Kunkiel-Kryńska A., *Prawo konsumenckie UE – dyrektywy oparte na metodzie harmonizacji minimalnej – wprowadzenie i wyrok TS z 16.05.1989 r. w sprawie 382/87 R. Buet i SARL Educational Business Services (EBS) v. Ministère public*, „Europejski Przegląd Sądowy" 2011, nr 12, s. 46–48; także: https://www.eversheds-sutherland.com/documents/global/poland/articles_pdf/pl/2011-12-01_eps_prawo_konsumenckie_ue_dyrekywy_oparte_na_harmonizacji_minimalnej_akunkiel.pdf [dostęp: 2 XII 2019].

Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process, https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf [dostęp: 2 XII 2019].

Piotrowska A., *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018, CeDeWu.

Raport „Płatności cyfrowe" 2019, Izba Gospodarki Elektronicznej, https://eizba.pl/wpcontent/uploads/2019/11/PLATNOSCI_CYFROWE_2019.pdf?fbclid=IwAR1ol9GL6K85vybNy5iwjoctd4k7YPFuT1rki_OpLjTwSqw1DFpGNkBoXBk [dostęp: 2 XII 2019].

Rekomendacja KNF dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe, Warszawa, listopad 2015 r., Komisja Nadzoru Finansowego, https://zarabiajnabankach.pl/wp-content/uploads/2016/07/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf [dostęp: 2 XII 2019].

Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Komisja Europejska, https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf [dostęp: 4 XII 2019].

Stanowisko w sprawie wydawania kart przepłaconych, z 10 lipca 2015 r., Komisja Nadzoru Finansowego, https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [dostęp: 2 XII 2019].

System hawala i finansowanie terroryzmu, http://www.nowastrategia.org.pl/system-hawala-i-finansowanie-terroryzmu [dostęp: 2 XII 2019].

UK FinTech. State of the Nation, T. Helm, A. Low, J. Townson (red.), 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf [dostęp: 2 XII 2019].

Umowa międzynarodowa i memorandum of understanding – charakterystyka i terminologia, https://pressto.amu.edu.pl/index.php/cl/article/viewFile/6437/6458 [dostęp: 2 XII 2019].

Akty prawne

Dyrektywa PE i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Dz. Urz. UE L 156 z 19 VI 2018 r., s. 43).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 25 maja 2015 w sprawie zapobiegania wykorzystywania systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz. Urz. UE L 141 z 5 VI 2015 r., s. 73).

Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz. Urz. UE L 267 z 10 X 2009 r., s. 7).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j: DzU z 2019 r. poz. 1115, ze zm.).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j.: DzU z 2019 r. poz. 659, ze zm.).

Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j.: DzU z 2018 r. poz. 2286, ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j.: DzU z 2019 r. poz. 2357).

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

Abstrakt

Badania pokazują, że najpopularniejszymi instrumentami płatniczymi są: karta płatnicza, rachunek bankowy z dostępem internetowym oraz konto w serwisie PayPal. Szybki rozwój techniki i digitalizacji płatności elektronicznych powodują, że już w momencie wydania aktów prawnych regulujących funkcjonowanie rynku finansowego w tym sektorze są one nieadekwatne do zmieniającej się rzeczywistości. Powoduje to podatność tego saktora na ryzyko wynikające z działalności przestępczej, w tym terrorystycznej. Wyzwania dla rynku płatności elektronicznych oraz organów nadzorczych w najbliższych latach będą się koncentrowały wokół przystosowania działalności do nowych trendów cyfrowych, implikacji związanych z rozwojem FinTech oraz RegTech, śledzeniu trendów i wyzwań w obszarze walut wirtualnych, wspieraniu wymiany informacji oraz współpracy pomiędzy instytucjami finansowymi a organami nadzorczymi, a także przeciwdziałaniu praktykom de-riskingu.

Słowa kluczowe: FinTech, RegTech, przeciwdziałanie praniu pieniędzy, przeciwdziałanie finansowaniu terroryzmu, AMC, CFT, EBA, KNF.

Abstract

Research shows that the most popular payment instrument is a payment card, then a bank account with Internet access and then a PayPal account. The progress and increase in the digitization of electronic payments means that when legislation is issued in these areas, they are no longer adequate to the changing reality. This makes them vulnerable to the risks associated with criminal activities, including terrorist activities. Challenges for the entire electronic payments market and supervisory authorities in the coming years will focus on adaptation to new digital challenges, implications related to the development of FinTech and RegTech, tracking trends and challenges in the area of virtual currencies, supporting information exchange

and cooperation between financial institutions and supervisory authorities and counteracting de-risking practices.

Keywords: FinTech, RegTech, anti money laundering, counter terrorist financing, AML, CFT, EBA, KNF.