Nr 1(94) 2024

eISSN 2544-7068

BEZPIECZNY BANK

SAFE BANK

BFG Bankowy Fundusz Gwarancyjny

BEZPIECZNY BANK jest czasopismem wydawanym przez Bankowy Fundusz Gwarancyjny od 1997 roku, poświęconym zagadnieniom stabilności systemu finansowego, ze szczególnym uwzględnieniem systemu bankowego.

Artykuły publikowane w BEZPIECZNYM BANKU są recenzowane.

Czasopismo BEZPIECZNY BANK znajduje się w Wykazie czasopism naukowych i wydawnictw MNiSW i MEiN (40 punktów).
BEZPIECZNY BANK eISSN 2544-7068
Wcześniejsze wydania BEZPIECZNEGO BANKU miały numer ISSN 1429-2939

REDAKCJA TECHNICZNA

Krystyna Kawerska

WYDAWCA

Bankowy Fundusz Gwarancyjny
ul. Ks. Ignacego Jana Skorupki 4
00-546 Warszawa

SEKRETARIAT REDAKCJI

Ewa Teleżyńska
Telefon: 22 583 08 78
e-mail: redakcja@bfg.pl

Informacje dotyczące wymogów formalnych i edytorskich dla autorów publikacji znajdują się na stronie: **www.ojs.bfg.pl**

DOM WYDAWNICZY ELIPSA

Opracowanie komputerowe:
Dom Wydawniczy ELIPSA
ul. Inflancka 15/198, 00-189 Warszawa
tel. 22 635 03 01, e-mail: elipsa@elipsa.pl,
www.elipsa.pl

W numerze

Contents

Od Redakcji

Globalny kryzys finansowy z pierwszej dekady XXI w. dowiódł, że kryzys w banku lub bankach i jego konsekwencje nie tylko dla sektora bankowego mogą się pojawić jak przysłowiowa burza w górach czy biały szkwał na jeziorze. Działo się tak zarówno wtedy, gdy infrastruktura regulacyjno-ostrożnościowa była relatywnie niedojrzała, jak i w warunkach stosunkowo rozwiniętych standardów bezpieczno-ściowych. Dzieje się tak, gdy strategie ukierunkowane na wzrost efektywności 'usypiają' czy choćby ograniczają czujność bankowych decydentów co do ryzyka, które w normalnych warunkach nie stanowi zagrożenia stabilności funkcjonowania. Drastycznie przypomniały o tym kryzysy w amerykańskich bankach na przełomie I i II kwartału 2023 r. Niestety, nie tylko lekceważenie klasycznego ryzyka może prowadzić do poważnych perturbacji i kosztów, bądź konieczności pomocy zewnętrznej, w tym błyskawicznych decyzji o gwarancjach dla deponentów przeciwdziałających runom na banki. Charakterystykę takiego scenariusza opartą na analizie kryzysu banków amerykańskich zawiera opracowanie otwierające numer 94, zredagowane przez Redakcję „Bezpiecznego Banku" na podstawie publikacji International Monetary Fund w serii Global Financial Stability Notes. Niestety, w warunkach postępu technologicznego oraz coraz groźniejszych ataków hakerskich rozwój bankowości cyfrowej generuje nowe ryzyka operacyjne, które mogą być niezależne od staranności banków. Chodzi zwłaszcza o przestępczość cybernetyczną, która naraża na straty nie tylko poszczególnych klientów, ale także banki. O tym pierwszym aspekcie traktuje opracowanie o phishingu w części *Problemy i poglądy*, natomiast o tym drugim sondaż diagnostyczny o świadomości cyberbezpieczeństwa w części *Miscellanea*.

W nurcie walki o uczciwe pośrednictwo finansowe i przeciwdziałanie praniu brudnych pieniędzy lokują się dwa teksty. Pierwszy o relacjach norm dyrektyw UE i prawa krajowego w zakresie ścigania przestępstw prania brudnych pieniędzy i drugi o możliwościach wymiany informacji w ramach zrzeszenia banków spółdzielczych na gruncie przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Kolejny artykuł traktuje sygnalnie o zagadnieniu dematerializacji listów zastawnych w kontekście zmian regulacyjnych, akcentując zarówno zalety, jak i wady tego rozwiązania.

W końcowej części *Problemy i poglądy* publikujemy rozważania *de lege lata* i *de lege ferenda* w kwestii etyki w świetle Rekomendacji Z KNF dotyczącej ładu wewnętrznego w bankach.

Z tej syntetycznej charakterystyki wynika, że numer 94 „Bezpiecznego Banku" w dominującej części jest poświęcony problematyce prawnej działalności banków. A swoistym domknięciem zamieszczonych w nim artykułów jest recenzja nader oryginalnej, a przede wszystkim instrukcyjnej, zwłaszcza dla środowiska prawniczego, książki K. Kalickiego i M. Jabłońskiego, poświęconej zaawansowanej anatomii problemu kredytów walutowych, której w modnej stylizacji można nadać logo *must read*.

Zachęcając do zapoznania się z przygotowanymi dla P.T. Czytelników opracowaniami, życzę interesującej lektury.

Jan Szambelańczyk
Redaktor Naczelny

Problemy i poglądy

DOI: 10.26354/bb.1.1.94.2024

Przyczyny, przebieg i konsekwencje kryzysu banków w USA na przełomie I i II kwartału 2023 roku*

Streszczenie

W ciągu kilku dni w marcu 2023 r. upadły trzy banki w USA, jako pierwszy upadł Silicon Valley Bank (SVB) 16. największy bank w USA, a następnie Signature Bank (SB) i First Republic Bank (FRB). Zdarzenia te przypomniały o upadku Washington Mutual Bank w 2008 r. Bezpośrednią przyczyną upadłości SVB, SB i FRB był gwałtowny odpływ depozytów, a to zwiększyło ryzyko podobnego runu na inne banki w amerykańskim sektorze bankowym. Dotyczyło to zwłaszcza tych banków, które miały stosunkowo duże udziały depozytów klientów nieobjętych gwarancjami FDIC, miały nierozliczone straty na aktywach albo portfele kredytowe miały znaczne ekspozycje na nieruchomości komercyjne. Procesy te jeszcze raz uświadomiły zagrożenia dla stabilności banków spowodowane zagregowanym oddziaływaniem zaostrzonej polityki pieniężnej i finansowej oraz niewłaściwego zarządzania odsetkami, płynnością i ryzykiem kredytowym. W opracowaniu poddano analizie sytuację finansową upadłych banków oraz średniookresową projekcję zagrożeń stabilności jaka może wystąpić w bankach o podobnym profilu działalności i strukturze bilansu[1].

Słowa kluczowe: FRB, SBNY, SVB, gwarantowanie depozytów, upadłość banków

Kody JEL: E40, E42, E43, G01, G21

* Tekst stanowi redakcyjne opracowanie na podstawie oryginału: GLOBAL FINANCIAL STABILITY NOTE, *The US Banking Sector since the March 2023 Turmoil: Navigating the Aftermath*, International Monetary Fund, March 2024, Note/2024/001, którego autorami są Tobias Adrian, Nassira Abbas, Silvia L. Ramirez i Gonzalo Fernandez Dionis.

1 Zgodnie z klasyfikacją nadzorczą FED banki: SVB, SBNY i FRB były uznawane za duże (ang. *large*) instytucje bankowe, według wartości ich bilansów. Natomiast uczestnicy rynku traktowali je jako banki ponadregionalne, mieszczące się pomiędzy bankami społeczności lokalnych a największymi bankami w USA (Por. *Federal Reserve Board – Approaches to Bank Supervision*).

Causes, Course and Consequences of the Bank Crisis in the USA at the Turn of the 1st and 2nd Quarter of 2023

Abstract

Within a few days in March 2023, three banks failed in the US, Silicon Valley Bank (SVB) the 16th largest US bank was the first to fail, followed by Signature Bank (SB) and First Republic Bank (FRB). These events recalled the 2008 collapse of Washington Mutual Bank. The immediate cause of the bankruptcy of SVB, SB and FRB was a rapid outflow of deposits, which increased the risk of a similar run on other banks in the American banking sector. This was particularly true for banks that had relatively large shares of customer deposits not covered by FDIC guarantees, had unsettled asset losses, or had significant exposures to commercial real estate in their loan portfolios. These processes have once again highlighted the threats to bank stability caused by the aggregate impact of tight monetary and financial policy and mismanagement of interest, liquidity and credit risk. The study analyzes the financial situation of bankrupt banks and the medium-term projection of stability threats that may occur in banks with a similar business profile and balance sheet structure.

Keywords: FRB, SBNY, SVB, deposit insurance, bank failure

JEL Codes: E40, E42, E43, G01, G21

Wykaz najważniejszych skrótów

AFS – dostępne do sprzedaży (ang. *available for sale*)
BTFP – Bankowy Program Finansowania Terminowego (ang. *Bank Term Funding Program*)
CRE – nieruchomości komercyjne (ang. *commercial real estate*)
FDIC – Federalna Korporacja Gwarantowania Depozytów (ang. *Federal Deposit Insurance Corporations*)
FHLB – Federalne Banki Pożyczek Domowych (ang. *Federal Home Loan Banks*)
FED – System Rezerwy Federalnej, Rezerwa Federalna (ang. *Federal Reserve System*)
FRB – First Republic Bank
HTM – utrzymywane do terminu zapadalności (ang. *held to maturity*)
KRI – kluczowy wskaźnik ryzyka (ang. *Key Risk Indicator*)
RMBS – papiery wartościowe zabezpieczone hipoteką na nieruchomościach mieszkalnych (ang. *residential morthage-backed securities*)
SBNY – Signature Bank of New York
SVB – Bank Doliny Krzemowej (ang. Silicon Valley Bank)

Słowo wstępne od Redakcji „Bezpecznego Banku”

Opracowanie IMF z marca 2024 r. dotyczące przede wszystkim przesłanek i konsekwencji upadłości trzech banków w USA, jakie miały miejsce w marcu 2023 r., zawiera oceny i wnioski – w zasadzie znane w teorii finansów i bankowości. Okazuje się jednak, że praktyka rynku finansowego, w jednym z największych i najbardziej konkurencyjnych systemów bankowych świata, mającym bogate doświadczenia z kryzysów o lokalnym, stanowym, federalnym czy nawet globalnym charakterze,

z rozwiniętą infrastrukturą regulacyjną, silnymi ogniwami sieci bezpieczeństwa finansowego, w tym instytucją gwarancyjną o najdłuższej historii, może zaskakiwać. Pomimo zaawansowanego systemu kontroli i nadzoru kryzys w banku pojawia się jak przysłowiowa burza w górach, zaskakując nie tylko turystów amatorów. Okazuje się bowiem, że zakumulowany wpływ rozwoju inżynierii finansowej wraz z bezprecedensowym tempem postępu technologicznego na rynkach finansowych potrafi generować nie tyle nowe co błyskawicznie materializujące się ryzyka i zagrożenia stabilności dla systemu finansowego. To z kolei wymaga zarówno posiadania scenariuszy szybkiego reagowania kryzysowego, jak i odwagi najważniejszych krajowych decydentów w niezwłocznym podejmowaniu koniecznych decyzji, nie zawsze dobrze przewidzianych w przepisach prawa. Można by tu odwołać się do znanego powiedzenia: *nie szkoda róż gdy płoną lasy*.

Publikując w „Bezpiecznym Banku" opracowanie przygotowane pod auspicjami IMF w serii „Global Financial Stability", Redakcja ma przede wszystkim na celu ostrzeżenie interesariuszy polskiego systemu finansowego, że nie mogą polegać na pozornie optymistycznych przesłankach stabilności, a ogniwa sieci bezpieczeństwa muszą być nieustannie gotowe nawet do nadzwyczajnych działań, w imię ochrony stabilności. Decyzja Prezydenta i Sekretarza Skarbu USA z 2023 r. o gwarancjach dla wszystkich depozytów w sytuacji ryzyka runu na banki może być przyczynkiem do polskiej debaty nad dylematami ochrony kredytobiorców walutowych kosztem pozostałej części klientów banków.

Warto także podkreślić wagę drugiej części prezentowanego niżej opracowania IMF, w której analizuje się nie to co się już zdarzyło, lecz to co się dopiero zdarzyć może ze względu na sytuację banków z tzw. 'słabego ogona' amerykańskiego systemu bankowego.

Wstęp

W marcu i kwietniu 2023 r. światowy system finansowy doświadczył najpoważniejszych napięć od czasu globalnego kryzysu finansowego pierwszej dekady XXI w. Upadek trzech amerykańskich banków, sklasyfikowanych jako duże instytucje finansowe, jaskrawo uwypuklił brak przygotowania do działalności w środowisku wyższych stóp procentowych, po relatywnie długim okresie niskiego ich poziomu. Między marcem 2022 r. a wrześniem 2023 r., w warunkach uporczywie wysokiej inflacji, FED podniósł efektywną stopę funduszy federalnych o 525 punktów bazowych. Był to najszybszy cykl zacieśniania polityki pieniężnej od lat 80. ubiegłego wieku[2]. Po latach wyjątkowo niskich stóp procentowych i luźnej polityce finansowej, zacieśnienie polityki pieniężnej w celu stłumienia inflacji do poziomu celu ujawniło zagrożenia w segmencie słabych finansowo (org. słabego ogona) banków,

[2] Federal Reserve Financial Stability Report, October 2023, s. 26, Financial Stability Report October 2023 (federalreserve.gov); and FDIC Quarterly, s. 46, FDIC Quarterly 2023, Vol 17, No 4, s. 46.

które wymagały zdecydowanych działań ze strony władz USA, aby zapobiec ryzyku, które zagroziłoby stabilności systemu bankowego.

Do powstania ówczesnych napięć w sektorze bankowym przyczyniło się kilka okoliczności. Jednak niektóre mogły być wcześniej dostrzeżone jako sygnały ostrzegawcze o kondycji banków w środowisku wyższych stóp procentowych. Niestety, pomimo jasnej komunikacji ze strony władz monetarnych, tempo i skala wzrostu stóp procentowych okazały się trudnym wyzwaniem dla instytucji finansowych, które nieodpowiednio zarządzały ryzykiem stopy procentowej i płynności, zbyt optymistycznie zakładając długość okresu wysokiej inflacji. W rzeczywistości bezprecedensowe wsparcie dla gospodarki udzielane podczas pandemii doprowadziło do nietypowego wzrostu oszczędności i depozytów bankowych, z których duża część została zainwestowana przez banki w papiery wartościowe o dłuższym terminie zapadalności. Były one także obarczone znacznym ryzykiem stopy procentowej. Początkowo silny wzrost kredytów i wolniejsze zmiany oprocentowania depozytów przyczyniły się do wzrostu marż netto. Jednak wraz ze wzrostem stóp procentowych banki stanęły w obliczu zwiększonych kosztów finansowania i spadku wartości rynkowej posiadanych papierów wartościowych. Spowodowało to gwałtowny wzrost niezrealizowanych strat na pasywach, utrzymywanych do terminu zapadalności (HTM) i aktywach dostępnych do sprzedaży (AFS). Ponadto deponenci zmienili swe preferencje i inwestowali w produkty o wyższej oczekiwanej stopie zwrotu, w tym fundusze rynku pieniężnego, co przyśpieszyło odpływ depozytów z banków. Na tym tle ryzyko duration – w trakcie cyklu zacieśniania polityki pieniężnej – negatywnie zweryfikowało doświadczenia korzystniejszej rentowności dla banków w warunkach relatywnie wysokich stóp procentowych.

Upadek SVB ujawnił zagrożenia strukturalne wynikające z modeli biznesowych niektórych amerykańskich banków, a pogorszone nastroje rynkowe doprowadziły do odpływu depozytów w niektórych instytucjach[3], co dodatkowo zwiększyło obawy inwestorów. Problemy stabilności sektora z marca 2023 r. udowodniły zwiększony wpływ postępu technologicznego, a zwłaszcza bankowości mobilnej i komunikacji elektronicznej, na błyskawiczne stymulowanie zachowań klientów, w tym większe ryzyko runu na bank lub banki[4]. W ciągu kilku dni upadły SVB i SBNY, co oznaczało drugą i trzecią co do wielkości upadłość banku w historii amerykańskiej bankowości dopóki nie upadł First Republic Bank. Napięcia w amerykańskim sektorze bankowym zwiększyły niepewność na rynku. Globalne rynki akcji zanotowały gwałtowny spadek i wzrost zmienności, a indeksy bankowe bardzo szybko straciły na wartości.

Zdecydowana reakcja decydentów politycznych w celu powstrzymania ryzyka systemowego pozwoliła uniknąć rozprzestrzeniania się kryzysu poprzez zapewnienie

[3] Banki o łącznych aktywach powyżej 250 mld USD znacząco zwiększyły wolumen depozytów w tym okresie, co świadczy o ich realokację z małych banków do dużych. Bank Rezerwy Federalnej Nowego Jorku, Liberty Street Economics, 11 maja 2023 r.

[4] O historycznych porównaniach upadłości zob. „Global Financial Stability Report: A New Look at Global Vulnerabilities"; (MFW 2023).

awaryjnej płynności i ochronę deponentów, a główną rolę odegrała Rezerwa Federalna, co pozwoliło uniknąć dysfunkcji rynku. Nowy instrument Bank Term Funding Program (BTFP) zapewnił bankom finansowanie po wartości nominalnej, bez marży stosowanej do kwalifikujących się zabezpieczeń, i przyczynił się do utrzymania zaufania do amerykańskiego systemu bankowego. Ponadto Federalna Korporacja Gwarantowania Depozytów (FDIC) zapewniła nieubezpieczonym deponentom SVB i SBNY gwarancje na podstawie klauzuli „wyjątku ryzyka systemowego". Biorąc pod uwagę powiązania systemu finansowego, upadek SVB udowodnił, że nawet instytucja finansowa nie mająca globalnego znaczenia systemowego może stanowić poważne zagrożenie dla stabilności.

Po zawirowaniach z marca 2023 r. amerykański sektor bankowy doświadczył ożywienia, choć sektor banków regionalnych w mniejszym stopniu[5]. Po perturbacjach wywołanych upadkiem SVB, zagregowane wskaźniki finansowe tego segmentu sektora wykazały poprawę. Do końca stycznia 2024 r. odpływ depozytów ustabilizował się, a indeks KBW Regional Bank Equity Index uległ poprawie. Utrzymują się jednak słabości w amerykańskim sektorze bankowym. Zmiany w oczekiwaniach dotyczących czasu i tempa obniżek stóp procentowych w USA, w połączeniu ze znacznymi stratami ogłoszonymi przez duży bank regionalny o silnych ekspozycjach na nieruchomości komercyjne (CRE), spowodowały 10-procentowy spadek powyżej wskazanego indeksu, potwierdzając, że zaufanie inwestorów do sektora pozostaje niestabilne. Utrzymują się także obawy wobec banków, które mają wysoki poziom niezrealizowanych strat powstałych w wyniku niedawnego wzrostu stóp procentowych i dużej potencjalnej presji na płynność depozytów nie objętych gwarancjami FDIC. Inne formy mniej stabilnego finansowania są szczególnie istotne dla banków o skoncentrowanej ekspozycji na CRE.

Przypadek SVB: Złożony i skoncentrowany model biznesowy przetestowany przez środowisko wyższych i dłuższych stóp procentowych

SVB zdefiniował się jako „partner finansowy" dla inwestorów w ekosystemie innowacji (*start-upy* i *venture capital*). Korzystając z ogromnej ekspansji sektora technologicznego, SVB niemal czterokrotnie zwiększył swoją wielkość w latach 2016–2023, z depozytami przekraczającymi 175 miliardów USD w porównaniu do 40 miliardów USD w 2016 roku (rys. A, panel 1). Bank był wyjątkowy pod wieloma względami. Po pierwsze, baza klientów była szczególnie jednorodna, a wolumen depozytów tworzyły głównie depozyty hurtowe o wysokiej koncentracji sektorowej (*start-up'y* i *venture capital*) oraz geograficznej w Dolinie Krzemowej w północnej Kalifornii. Wartość 86% ogółu depozytów przekraczała maksymalny poziom gwarancji. Po drugie, kierownictwo banku skoncentrowało inwestycje pochodzące z depozytów w długoterminowe papiery wartościowe zabezpieczone hipotekami mieszkaniowymi (RMBS), które były narażone na ryzyko stopy procentowej. Po trzecie, wzmocniony nadzór i wymogi regulacyjne dla dużych banków nie miały zastosowania do SVB lub zostały zastosowane dopiero wtedy gdy zidentyfikowano jego gwałtowny i niebezpieczny wzrost. Po czwarte, dostęp SVB do okna dyskontowego Rezerwy Federalnej nie był aktywny operacyjnie.

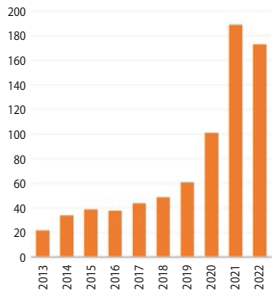
[5] Klasyfikacja banków w omawianym opracowaniu jest zgodna z definicją nadzorczą FED. Małe banki aktywa poniżej 10 mld USD, banki regionalne od 10 do 100 mld USD, duże banki powyżej 100 mld USD.

Pod koniec 2022 r. i na początku 2023 r. spowolnienie działalności w sektorze wysokich technologii spowodowało wycofywanie depozytów, bez ekwiwalentu napływu funduszy do banku ze strony innych podmiotów z tego sektora. Wraz ze wzrostem wolumenu niezrealizowanych strat SVB stał się narażony na nagłe ryzyko utraty płynności, którego nie uwzględniono w zarządzaniu ryzykiem i kierowaniem bankiem. Na początku marca 2023 r. plan pozyskania kapitału w ramach restrukturyzacji bilansu nie powiódł się. Wiadomość ta wywołała obawy deponentów i szybko przekształciła się w run na bank. 42 miliardy USD depozytów wypłynęło z banku 9 marca, a kolejne 100 miliardów miało wypłynąć następnego dnia, co oznaczało najszybszy i największy run na depozyty w tym stuleciu (rys. A, panel 3). Dodatkowo na koniec 2022 r., niezrealizowane straty SVB wynosiły 104% kapitału Tier 1. W tych okolicznościach 10 marca Kalifornijski Departament Ochrony i Innowacji Finansowych zamknął SVB, a Federal Deposit Insurance Corporation została wyznaczona na syndyka masy upadłościowej.

Rysunek A. Szybko rosnące depozyty, duży udział depozytów nieubezpieczonych i najszybszy bieg depozytów

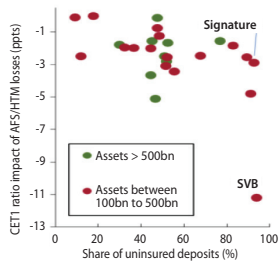
Gwałtowny wzrost depozytów

1. Depozyty ogółem
(w mld USD)



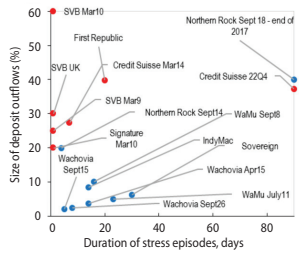
Niezrealizowane straty i struktura depozytów

2. Straty na CET1 w 4Q2022
(w %)



Najszybszy i największy run na depozyty

3. Run na depozyty
(% depozytów ogółem i liczba dni)



Źródło: Ennis and Keister 2009; Federal Deposit Insurance Corporation 1997; Federal Reserve, bank financial reports; Investigation Commission of Althing 2010; Kobrin 2011; Levy-Yeyati, Martinez Pería, and Schmukler 2010; Nakaso and Hattori 2002; Nascimento 1991; Northern Rock Applicants v Caldwell & HM Treasury (UKUT 408, 2011); Rose 2015; Schumacher 2000; Shin 2009; Simorangkir 2011; and IMF staff calculations.

Efekt domina: Signature Bank of New York i First Republic Bank

Upadek SVB wywołał szeroką debatę o stabilności amerykańskiego systemu bankowego. Inwestorzy zaczęli oceniać płynność i wypłacalność innych banków z uwzględnieniem redukcji wartości ich aktywów, w szczególności papierów wartościowych utrzymywanych do terminu zapadalności (rys. B, panel 2) i kredytów CRE, przy jednoczesnym założeniu, że niegwarantowane depozyty stały się niestabilne.

Signature Bank of New York – SBNY o aktywach wartości 110 mld USD, z dużą ekspozycją na niestabilne aktywa kryptowalutowe i wysokim udziałem niegwarantowanych depozytów (90%), szybko został zarażony i stał się obiektem runu na bank, niemal natychmiast po upadku SVB. Pod koniec 2022 r., SBNY miał koncentrację CRE, na poziomie 334% kapitału Tier 1 a niezrealizowane straty w stosunku do kapitału Tier 1 w wysokości 32%. Departament Usług Finansowych Stanu Nowy Jork i FDIC zamknęły Bank 12 marca po tym, jak w ciągu kilku dni stracił ponad 70% kapitału własnego.

First Republic Bank – FRB, z aktywami o wartości 212 miliardów USD, koncentrował się na zamożnych klientach indywidualnych. Jego model biznesowy zapewniał preferencyjne długoterminowe oprocentowanie dla tych klientów. W zamian zarządzał ich majątkiem, głównie poprzez przechowywanie wysokich oszczędności przekraczających sumy gwarancyjne FDIC. Prawie połowa portfela kredytowego dotyczyła hipotek na nieruchomościach mieszkalnych, które straciły znaczną część wartości na skutek przeszacowania wynikającego ze wzrostu stóp procentowych.

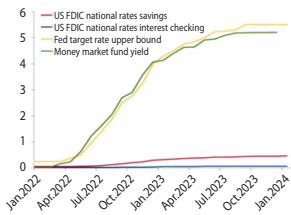
16 marca 2023 r. konsorcjum 11 publicznie notowanych banków pod przewodnictwem JPMorgan Chase zdeponowało 30 miliardów USD w FRB, aby zwiększyć płynność i dać rynkowi silny sygnał o wsparciu dla amerykańskiego sektora bankowego. Jednak nastroje klientów co do stabilności FRB nie poprawiły się, co doprowadziło do zamknięcia banku przez Kalifornijski Departament Ochrony i Innowacji Finansowych. Pod koniec marca 2023 r., niegwarantowane depozyty w FRB stanowiły 49% wszystkich depozytów, koncentracja CRE wynosiła 209% kapitału Tier 1, a niezrealizowane straty w kapitale Tier 1 wynosiły 30%. Wraz z zamknięciem FRB FDIC została syndykiem masy upadłościowej, a JPMorgan Chase nabył wszystkie rachunki depozytowe i prawie wszystkie aktywa z datą 1 maja 2023 r. Upadłość FRB była drugą co do wartości upadłością banku w historii USA i największą od czasu upadku Washington Mutual Bank w 2008 r. (rys. B, panel 3).

Po zawirowaniach z marca 2023 r. amerykański sektor bankowy pozostaje pod uważną obserwacją uczestników rynku. I choć banki są obecnie znacznie bardziej dokapitalizowana niż podczas globalnego kryzysu finansowego, głównie na skutek międzynarodowych reform regulacyjnych, inne słabości pozostają. Przykładowo, różnica między stopami procentowymi a cenami depozytów pozostaje duża, wywierając presję na koszty finansowania i marże. W 4Q2023 łączna wartość niezrealizowanych strat w bilansach amerykańskich banków wynosi 477 mld dolarów (rys. B, panel 2).

Rysunek B. Odpływ depozytów i mniejsza płynność, szczególnie dla banków regionalnych

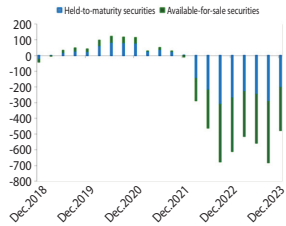
Gdy stopy procentowe gwałtownie wzrosły oprocentowanie rosło wolniej

1. Wybrane benchmarki
(w %)



ale banki w USA miały niezrealizowane straty na papierach wartościowych

2. Niezrealizowane zyski i straty na papierach wartościowych w sektorze bankowym w USA
(w mld USD)



FRB był największym upadłym bankiem po WMB w 2008 r.

3. Dziewięć największych upadłych banków w USA według aktywów
(w mld USD)

Name	Date of failure	Total assets
Washington Mutual	2008	307
First Republic Bank	2023	233
Silicon Valley Bank	2023	212
Signature Bank of New York	2023	110
Continental Illinois National Bank and Trust	1984	40
IndyMac	2008	31
American Savings and Loan Association	1988	30
Colonial bank	2009	26
Guaranty Bank	2009	14

Źródło: American Banker "Hall of Shame: 10 biggest bank failures", Bloomberg LP, Crane, Federal Reserve and Federal Deposit Insurance Corporation.

Wstrząs na rynkach finansowych w następstwie upadłości Silicon Valley Bank

Wstrząs na rynkach finansowych spowodowany upadłością SVB był najsilniejszy od czasu globalnego kryzysu finansowego. Ceny akcji małych i regionalnych banków gwałtownie spadły. Zmienność rynku gwałtownie wzrosła. Niepokoje szybko przeniosły się na rynek finansowania krótkoterminowego, powodując nagłe zaostrzenie warunków finansowych (rys. C, panele 1 i 2). Zawirowania na rynku bankowym doprowadziły również do nagłej ucieczki w kierunku jakości na rynku obligacji państwowych i bezprecedensowego przeszacowania oczekiwań dotyczących stóp rynkowych.

W przeciwieństwie do kryzysu subprime z 2008 r. turbulencje po marcu 2023 r. były znacznie bardziej ograniczone. Niemniej jednak inwestorzy pozostali szczególnie ostrożni w stosunku do banków regionalnych, które odgrywają istotną rolę w finansowaniu przedsiębiorstw i sektora nieruchomości komercyjnych.

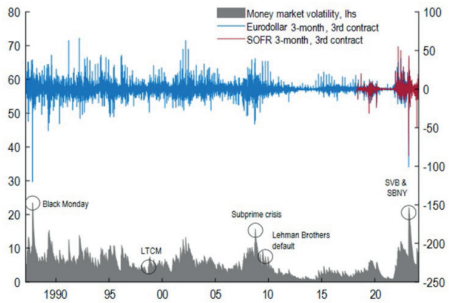
Obawa przed szerszym rozprzestrzenianiem się kryzysu była najważniejsza dla decydentów politycznych od początku zawirowań z marca 2023 roku. Aby powstrzymać dalsze skutki, amerykańskie organy nadzoru finansowego wprowadziły wiele odważnych środków. Władze USA[6] ogłosiły 12 marca 2023 r. gwarancję dla depozytów SVB i Signature Bank of New York (SBNY), bez limitu ich wysokości wykorzy-

[6] Sekretarz Skarbu, w porozumieniu z Prezydentem USA, zatwierdzili wyjątek systemowy. Zob. komunikat we wspólnym oświadczeniu Departamentu Skarbu, Rezerwy Federalnej i FDIC: https://www.fdic.gov/news/press-releases/2023/pr23017.html.

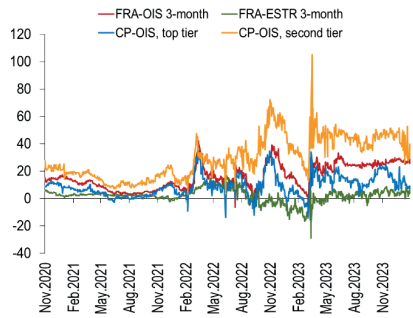
stując formułę wyjątku od ryzyka systemowego[7]. Rynki poczuły się uspokojone, że amerykańskie organy regulacyjne zrobią „wszystko, co w ich mocy", aby zapobiec szerszemu zarażeniu.

Rysunek C. Rynki finansowe i zawirowania na rynku bankowym w latach 1980–2023

1. Krótkoterminowe zmiany oczekiwań polityki monetarnej w USA vs główne zdarzenia ryzyka
(w punktach bazowych)



2. Finansowanie międzybankowe w USA i w strefie euro
(w punktach bazowych)

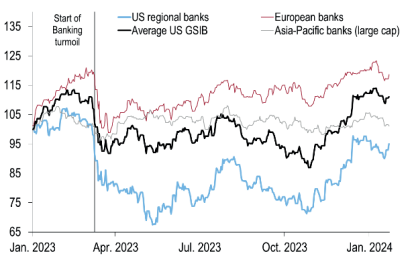


Uwaga: CP= US commercial paper index; CP-OIS = CP- OIS; FRA-OIS= FRA-OIS; FRA-ESTR= FRA-ESTR;
FRA = Forward rate agreement;
ESTR= Euro short-term rate;
OIS= Overnight index swap;
LTCM = Long-Term Capital Management;
SOFR = Secured overnight financing rate.

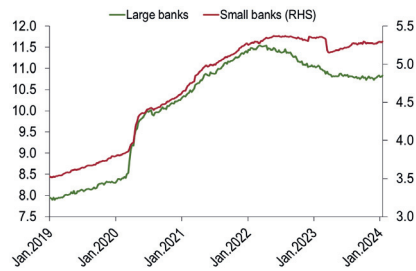
Źródło: Bloomberg Finance L.P., Federal Reserve, and IMF obliczenia własne.

Rysunek D. Indeksy akcji banków i depozyty amerykańskich banków

1. Wybrane indeksy giełdowe
(1 stycznia 2023 r. = 100)



2. Depozyty bankowe w USA
(w bln USD)



Uwaga: US Regional Banks index dotyczy KBW Bank Index, który obejmuje banki o wartości aktywów od 10 do 110 mld;
GSIB = Global systemically important bank.

Źródło: Bloomberg Finance L.P., Federal Reserve, and IMF obliczenia własne.

[7] Komunikat prasowy FDIC: PR-17-2023 3/12/2023.

Ponadto FED niezwłocznie wprowadził tymczasowy instrument płynnościowy, BTFP, który zapewnia amerykańskim instytucjom depozytowym alternatywę dla okna dyskontowego w celu wzmocnienia swojej roli pożyczkodawcy ostatniej instancji. 15 marca 2023 r. banki pożyczyły 12 miliardów dolarów. Pożyczki mają dłuższe terminy niż operacje okienka dyskontowego i mogą być przedłużane do jednego roku przy oprocentowaniu równym stopie swapowej indeksu overnight powiększonej o 10 punktów bazowych (stałej przez cały okres trwania zaliczki). Bardzo atrakcyjne warunki tego instrumentu pozwoliły wygenerować płynność, aby zapewnić bankom „zdolność do zaspokojenia potrzeb wszystkich deponentów" bez sprzedaży papierów wartościowych i zrealizowania strat rynkowych spowodowanych wyższymi stopami procentowymi. Program miał działać do marca 2024 r. Po 15 marca 2023 r. kwota pożyczek rosła, osiągając 20 lutego 2024 r. 165 miliardów dolarów. Wzrost ten wynika głównie z atrakcyjności oprocentowania, co prowadzi do pewnego arbitrażu z oprocentowaniem rezerw. 24 stycznia 2024 r. FED ogłosiła dolną granicę oprocentowania nowych pożyczek BFTP, aby ich oprocentowanie równe było oprocentowaniu rezerw[8].

Projekcja sytuacji w amerykańskim sektorze bankowym

Przed upadłością SVB, SBNY i FRB miały wysoki udział depozytów niegwarantowanych przez FDIC, znaczne niezrealizowane straty i/lub wysoką koncentrację kredytów na nieruchomości komercyjne. Ich upadłość SVB miała wpływ na inne duże banki, co spowodowało natychmiastowe zainteresowanie inwestorów szerszą grupą banków, które również stanęły przed wyzwaniami związanymi z wysokimi stopami procentowymi.

W marcu 2023 r., po upadku SVB i SBNY, deponenci i inwestorzy zaczęli się martwić, najpierw o płynność, a następnie o kondycję finansową banków o podobnym profilu biznesowym, które: (1) doświadczały znacznego odpływu depozytów; (2) miały wysoki udział niegwarantowanych depozytów; (3) polegały na pożyczkach i wyższym wykorzystaniu instrumentów płynnościowych; (4) miały znaczne niezrealizowane straty; oraz (5) wysoką ekspozycją na CRE. Jakkolwiek atrybuty (1) i (2) były specyficzne dla upadłych instytucji (SVB, SBNY i FRB), w dalszych partiach zidentyfikowano grupę małych lub regionalnych banków, które mają podobną charakterystykę.

Przepływy depozytów

Po wybuchu pandemii COVID-19 w okresie niskich stóp procentowych depozyty bankowe gwałtownie wzrosły. W 1Q2020 depozyty odnotowały największy kwartalny wzrost od wczesnych lat 80. Do gwałtownego wzrostu depozytów przyczyniły

[8] W dniu 24 stycznia 2024 r. Rada Gubernatorów Rezerwy Federalnej ogłosiła zakończenie BTFP z dniem 11 marca 2024 r. zgodnie z wcześniej przyjętym harmonogramem.

się m.in.: (1) płatności gotówkowe w ramach bodźców fiskalnych mających na celu pobudzenie gospodarki; (2) wysoka stopa oszczędności osobistych; (3) tworzenie depozytów w ramach programu skupu aktywów FED; oraz (4) wycofanie komercyjnych i przemysłowych linii kredytowych. Do końca 2021 r. wartość depozytów w USD była o 39% wyższa niż przed pandemią. Wraz ze wzrostem stóp procentowych koszty depozytów rosły powoli, a depozyty spadały w 2022 roku. Trend ten przyspieszył w 1Q 2023, gdy koszt alternatywny utrzymywania depozytów wzrósł z powodu znacznie lepszych zysków z funduszy inwestycyjnych rynku pieniężnego. Ponadto obawy o wypłacalność niektórych instytucji bankowych również doprowadziły do odpływu depozytów, a dane kwartalne wykazały największy spadek. Około 11% analizowanych banków doświadczyło odpływu niegwarantowanych depozytów, przekraczając 5% całkowitych depozytów w 1Q 2023, przy czym dominowały w tym banki regionalne. W przeciwieństwie do banków regionalnych, banki powyżej 250 miliardów dolarów w marcu 2023 r. doświadczyły napływu depozytów, co sugeruje realokację depozytów z małych banków do dużych banków w okresie napięć[9].

Szybka interwencja rządu i dostępność instrumentów finansowania przywróciły zaufanie do sektora bankowego. W 2Q2023 depozyty ustabilizowały się na poziomie 18,6 mld USD, ponieważ małe i regionalne banki zwiększyły depozyty (rys. D, panel 2). W 4Q2023 w porównaniu z 2Q2023 depozyty wzrosły o 1% do 18,7 bln USD.

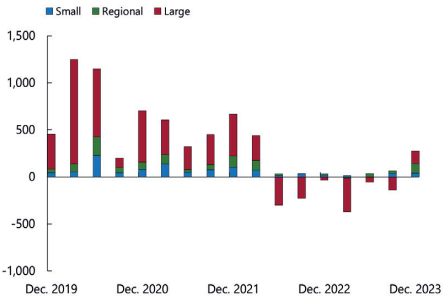
Zwiększona zależność banków od innych źródeł pożyczek

W sytuacji zagrożenia utratą płynności banki poszukiwały innych źródeł pożyczek jako środka zapobiegawczego, aby mitygować obawy inwestorów i zabezpieczyć swoją płynność na okoliczność zwiększonej zmienności ich bazy depozytowej. Zwróciły się więc o zaliczki z Federalnych Banków Pożyczek Domowych (FHLB), zaciągały kredyty z okna dyskontowego Rezerwy Federalnej i programu pożyczek awaryjnych oraz depozytów brokerskich. W 1Q2023, po upadku SVB, kredyty FHLB wzrosły gwałtownie, szczególnie w bankach regionalnych i dużych bankach. Podobnie rosły pożyczki, gdy banki uzyskały dostęp do BTFP. Jednak pożyczki spoza FHLB wzrosły bardziej w bankach regionalnych niż w małych i dużych. Świadczy to o tym, że banki regionalne były głównymi beneficjentami BTFP. Mediana wskaźnika całkowitego zadłużenia, obejmującego kredyty FHLB i kredyty spoza FHLB, wzrosła bardziej w przypadku banków regionalnych i dużych w porównaniu z małymi bankami (rys. E, panel 2).

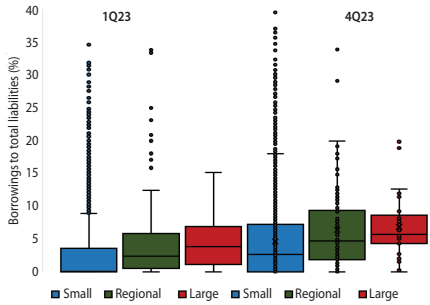
[9] Bank Rezerwy Federalnej Nowego Jorku, Liberty Street Economics, 11 maja 2023 r.

Rysunek E. Kwartalne zmiany depozytów i pożyczek, struktury oraz mediany niezrealizowanych strat banków regionalnych

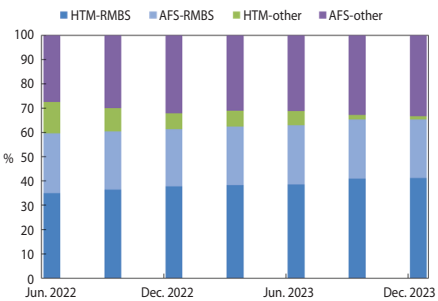
1. Kwartalna zmiana stanu depozytów
(w mld USD)



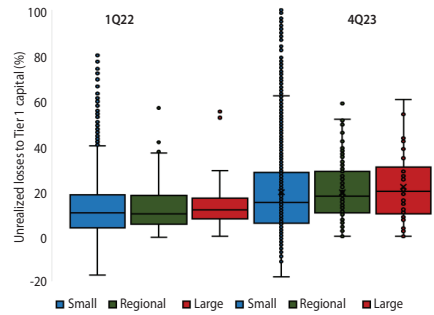
2. Mediana zadłużenia do zobowiązań ogółem
(w %)



3. Struktura niezrealizowanych strat
(w % ogółu niezrealizowanych strat)



4. Mediana niezrealizowanych strat do kapitału Tier 1 (w %)



Uwaga: W panelu 2 inne rodzaje pożyczek obejmują wszystkie inne długi z wyjątkiem zaliczek FHLB.
W panelach od 2 do 4 wykorzystano dane 4528 banków (tj. 98% banków posiadającymi gwarancje depozytów, mających w 3Q2023 99,8% aktywów banków ogółem.
W panelu 2 finansowanie niezwiązane z podstawową działalnością obejmuje pożyczki FHLB i inne pożyczone środki.
W panelu 3 AFS other obejmuje inne papiery niż RMBS.

Źródło: Bloomberg LP, S&P Capital IQ Pro, IMF szacunki własne

W miarę wzrostu stóp procentowych zmiany wartości portfeli RMBS prowadziły do wyższych niezrealizowanych strat. W 3Q2023 niezrealizowane straty w stosunku do kapitału Tier 1 pozostały na podwyższonym poziomie.

Niezrealizowane straty

Banki zareagowały na wzrost płynności wynikający z wyższego poziomu pozyskanych depozytów po pandemii, inwestując w długoterminowe papiery wartościowe o stałej stopie procentowej, w szczególności RMBS. Gdy stopy procentowe gwałtownie wzrosły w latach 2022 i 2023, wartość rynkowa posiadanych papierów wartościowych, klasyfikowanych jako HTM i AFS, znacznie spadła, co doprowadziło do dużych niezrealizowanych strat w bilansach banków. Papiery wartościowe typu HTM są wykazywane według zamortyzowanego kosztu, a niezrealizowane straty nie są generalnie odzwierciedlane w kapitale własnym lub kapitale regulacyjnym. Natomiast papiery wartościowe typu AFS są wykazywane według godziwej wartości rynkowej, a niezrealizowane z nich zyski lub straty są odzwierciedlane w kapitale własnym i kapitale regulacyjnym niektórych banków[10].

Niezrealizowane straty z tytułu posiadanych RMBS stanowiły prawie dwie trzecie ogółu niezrealizowanych strat i były wynikiem wzrostu oprocentowania kredytów hipotecznych. W okresie od 1Q2022 do 4Q2023, 30-letnia średnia krajowa stała stopa procentowa wzrosła o 209 punktów bazowych (rys. 3, panel 3). Niezrealizowane straty nadal rosły wraz ze wzrostem stóp procentowych i pozostały na wysokim poziomie 477 mld USD w 4Q2023, nawet po znacznym przeszacowania stóp terminowych w grudniu 2023 r. (rys. C, panel 2). Mediana wskaźnika niezrealizowanych strat do kapitału Tier I była wysoka, a między bankami występowały duże rozbieżności (rys. E, panel 4).

Pogorszenie warunków finansowych niektórych amerykańskich banków z tytułu znacznej ekspozycji na nieruchomości komercyjne

Pomimo znacznego ożywienia w amerykańskim sektorze bankowym po zawirowaniach z marca 2023 r. spora podgrupa instytucji nadal boryka się z poważnymi wyzwaniami. Podstawowe niepokoje utrzymują się, a ponadto są obawy, że upadek jednej instytucji może być akceleratorem szerszej utraty zaufania do sektora. Poza niezrealizowanymi stratami ryzyko kredytowe, a zwłaszcza ekspozycja na CRE niektórych instytucji, jest w centrum uwagi inwestorów. Małe i regionalne banki są w znacznym stopniu narażone na około dwie trzecie z 3 bilionów dolarów ekspozycji na CRE w amerykańskim systemie bankowym (rys. F, panel 1). Wysoka koncentracja ekspozycji na CRE stanowi poważne ryzyko dla małych i dużych banków w obliczu niepewności gospodarczej i wyższych stóp procentowych, potencjalnie spadających wartości nieruchomości i pogorszenia jakości aktywów. W 4Q2023 w tej grupie banków utrzymywała się wyjątkowo wysoka koncentracja CRE, w przypadku której straty mogłyby zagrozić stabilności[11].

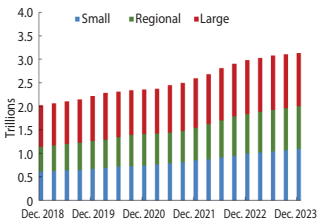
[10] Zob. Press release: FDIC: PR-55-2023 7/27/2023.

[11] Kryteria opracowane na podstawie wytycznych nadzorczych, uznają wysoką koncentrację za stosunek ekspozycji CRE do całkowitego kapitału opartego na ryzyku większym niż 300%. Managing Commer-

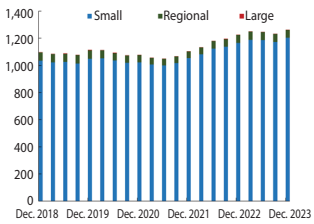
W miarę jak sektor nieruchomości komercyjnych zmaga się ze spadającymi cenami nieruchomości i rosnącymi wskaźnikami pustostanów, wskaźnik kredytów zagrożonych CRE dla amerykańskich banków do końca 2023 r. podwoił się, osiągając 0,81% z zaledwie 0,41% na koniec 2022 r. Przy czym duże banki odnotowały większy wzrost (+153 punkty bazowe) w porównaniu z małymi (+44 punkty bazowe) i regionalnymi bankami (+49 punktów bazowych). W ciągu ostatniego roku banki nadal zwiększały rezerwy na kredyty zagrożone CRE, choć w wolniejszym tempie niż wzrost samych kredytów zagrożonych. W rezultacie wskaźnik pokrycia CRE – stosunek rezerw na pokrycie przyszłych strat kredytowych do kredytów zagrożonych – spadł z 200% do 154% dla sektora bankowego. Spadek ten jest wyraźniejszy w przypadku amerykańskich banków o znaczeniu systemowym w porównaniu z pozostałymi. Pomimo tego spadku, wskaźnik pokrycia pozostaje stosunkowo wysoki, może wskazywać, że banki spodziewają się dodatkowych przypadków niewykonania zobowiązań. Tym bardziej, że są przesłanki, aby oczekiwać dalszego wzrostu kredytów zagrożonych w USA w nadchodzących kwartałach. Kwartalne wskaźniki kredytów zagrożonych CRE i straty nie osiągnęły szczytowego poziomu po dziewięciu kwartałach od rozpoczęcia globalnego kryzysu finansowego w połowie 2007 roku[12].

Rysunek F. Koncentracja kredytów na nieruchomości komercyjne (CRE)

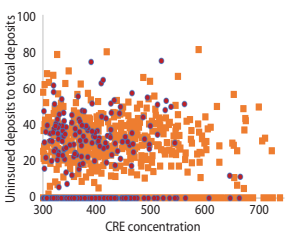
1. Ekspozycje CRE
(w bln USD)



2. Banki według wielkości z udziałem CRE powyżej regulacyjnego 300%
(liczba)



3.Banki regionalne z niezrealizowanymi stratami > 25% Kapitału Tier 1
(w %)



Uwaga: Rysunek w panelu 1 na podstawie danych nadzorczych;
Panele 2 i 3 zob. początkową uwagę do rysunku 3.
Czarne punkty na panelu 3 ilustrują pozycje banków regionalnych

Źródło: Bloomberg LP, S&P Capital IQ Pro, and IMF szacunki własne.

cial Real Estate Concentrations, July 10, 2023. FDIC: Managing Commercial Real Estate Concentrations – Winter 2007, Vol. 4, Issue 2. Jedna trzecia amerykańskich banków, głównie małych i regionalnych, posiadała ekspozycje na CRE przekraczające 300% ich kapitału powiększonego o odpis na straty kredytowe, co stanowi 16% aktywów ogółem systemu bankowego (rys. 4, panel 2). W ramach tych kategorii udział banków regionalnych o wysokiej koncentracji CRE przekracza 50%, małych banków 32% i dużych banków 3%. Ponadto ponad 100 banków, które stanowią około 3% aktywów systemu bankowego, ma wysoką koncentrację CRE, niezrealizowane straty przekraczające 25% kapitału Tier 1 i nieubezpieczone depozyty do depozytów ogółem przekraczające 25% (rys. 4, panel 3).

12 Na podstawie FDIC QBP Times Series Spreadsheet, Balance Sheet, FDIC: Quarterly Banking Profile.

Rynkowa wycena amerykańskiego sektora bankowego

Rynkowe wyceny banków amerykańskich pozostają na poziomie dyskonta w porównaniu z wycenami ze stycznia 2023 r. (rys. G, panel 1). Średnie wartości wskaźnika cena do wartości księgowej dla indeksu KBW Regional Bank Index[13] ucierpiały z powodu niepewności co do średnioterminowych perspektyw ich obecnych modeli biznesowych, a możliwość zaostrzenia regulacji i wzrostu wymogu kapitałowego zwiększa niepewność i odstrasza inwestorów. Bardzo dobrym przykładem jest gwałtowne pogorszenie się konsensusu prognostycznego dotyczącego przyszłej rocznej stopy zwrotu z kapitału własnego, która obniżył się poniżej 9% i jest znacznie niższy niż w przypadku porównywalnych spółek (rys. G, panel 2).

Aby zidentyfikować najsłabszy segment banków[14] wykorzystano metodę kluczowych wskaźników ryzyka[15] w stosunku do instytucji notowanych na giełdzie. Podejście to zostało wykorzystane do monitorowania w czasie rzeczywistym przyszłych zagrożeń poprzez uwzględnienie krótkoterminowych prognoz analityków bilansu banku, wyceny i wskaźników rentowności dla około 200 banków notowanych na giełdzie. Wskaźniki te lub kluczowe wskaźniki ryzyka (KRI) zostały wybrane ze względu na ich zdolność do przewidywania napięć finansowych w poszczególnych bankach i poważnych zdarzeń stresowych, jak duże spadki cen akcji lub odpływ depozytów[16].

Istnieją przesłanki wskazujące, że liczba banków w USA znajdujących się pod obserwacją pozostanie na wyższym poziomie niż zwykle, chociaż i tak zmniejszyła się od początku pandemii (rys. G, panel 3). Według oceny na 4Q2023 słaby segment ('słaby ogon') banków, szacuje się na 5,5 bln USD aktywów, co stanowi ca 23% całkowitych aktywów banków w USA.

[13] KBW Regional Index obejmuje aktualnie szeroką grupę banków o aktywach od 10 do 110 mld USD. Jeżeli wyłączyć NYCB, drugi co do wielkości bank ma sumę aktywów o wartości 75 mld USD.

[14] W opracowaniu IMF używa się często określenia *weak tail of banks* ('słaby ogon banków').

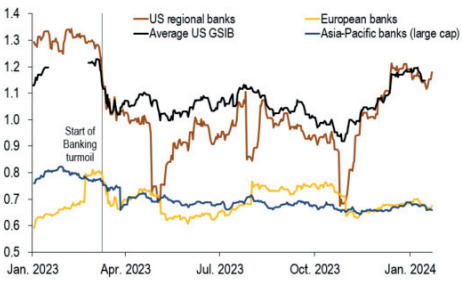
[15] Rozdział pt. *A New Look at Global Banking Vulnerabilities* w „Global Financial Stability Report" October 2023.

[16] Banki są identyfikowane, jeśli mają cechy odstające w wielu wymiarach, a tym samym są narażone na podwyższone ryzyko poważnych napięć. Ponieważ takie przypadki są rzadkie, wskaźniki KRI nie służą do prognozowania upadłości banków z wysokim prawdopodobieństwem. Zamiast tego stanowią one ważne narzędzie do śledzenia ogólnego poziomu napięć w globalnym systemie bankowym w czasie oraz do identyfikowania banków zasługujących na dokładniejsze zbadanie pod kątem oznak słabości.

Rysunek G. Banki zakwalifikowane do 'słabego ogona' mają atrybuty większości wymiarów ryzyka KRI

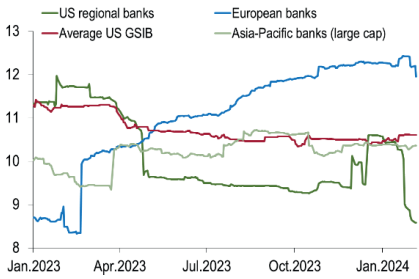
Wycena banków pozostaje z dyskontem w stosunku do 1Q2023 ze względu na poziom niepewności

1. Cena do wartości księgowej
(Price to book)



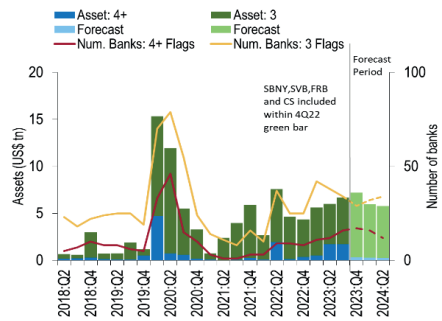
Konsensus prognostyczny wartości RoE dla banków regionalnych w USA dramatycznie obniżył się

2. Prognozowana roczna stopa zwrotu z kapitału własnego
(Bloomberg consensus one-year forward EPS/equity)



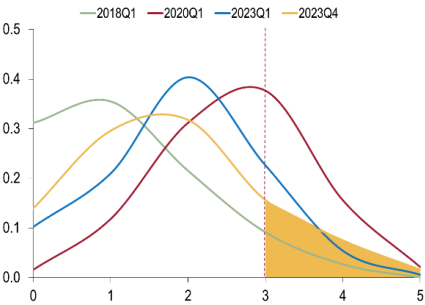
W 2024 r. liczba amerykańskich banków na ogólnej liście obserwacyjnej pozostaje podwyższona

3. Informacje banków odnośnie do składowych Kluczowego wskaźnika ryzyka



Aktualny rozkład banków z 4 i 5 słabymi atrybutami wykazuje większą ich liczbę

4. Distribution Densities for Flagged Banks
(Number of banks)



Przerywana pionowa linia dotyczy większości KRI

Uwaga: Dane paneli 3 i 4 wykorzystują dane historyczne od 1Q2018 do 4Q2023, w przypadku braku danych wykorzystano consensus prognostyczny dla 4Q2023, podobnie dla 1Q2024 I 2Q2024.
CS = Credit Suisse; GSIB= Global systemically important bank

Źródło: Bloomberg Finance L.P., Visible Alpha, and IMF obliczenia własne.

Podsumowanie

Upadłości banków w Stanach Zjednoczonych w 2023 r. uwidoczniły wiele słabości, które zagrażały stabilności krajowego sektora bankowego i nawet globalnej stabilności finansowej. Uwypukliły także te aspekty działalności, które powinny być odpowiednio zaadresowane przez decydentów politycznych, organy regulacyjne i nadzoru, a przede wszystkim bankowców zarządzających ryzykiem zarówno w ujęciu ram regulacyjnych, jak i nowych technologii kreujących zmieniony kontekst działalności i realizacji transakcji w czasie i przestrzeni. Jednak kluczowym problemem pozostaje nieodpowiedzialne i nadmierne podejmowanie ryzyka[17].

Doświadczenia i analizy pozwalają zidentyfikować luki w infrastrukturze regulacyjnej i nadzorczej, a także brak odpowiednich sankcji. Regulatorzy i nadzorcy muszą być w stanie wymagać od banków spełnienia wyższych niż minimalne standardów, gdy wymaga tego ryzyko; przydzielać odpowiednie zasoby mniejszym bankom, w których może występować ryzyko; zapewniać skuteczne procesy podejmowania decyzji i ich eskalację; oraz mieć nadwyżki specjalistycznych kompetencji.

Turbulencje w systemie bankowym w USA z 2023 r. kosztownie uwidoczniły wpływ gwałtownie rosnących stóp procentowych na stabilność finansową. Pokazały one również, w jaki sposób segment słabych banków (‘słaby ogon sektora’), nawet jeśli nie mają one charakteru systemowego, może wymusić na decydentach podjęcie nadzwyczajnych działań w celu ograniczenia rozprzestrzeniania się kryzysu na zdrowe banki.

Amerykański FED podjął kroki w celu wzmocnienia działań nadzorczych z uwzględnieniem wniosków z upadłości dużych banków i nadzoru nad SVB. Działania te obejmują poprawę nadzoru nad ryzykiem płynności i stóp procentowych poprzez przeprowadzanie docelowych przeglądów w bankach wykazujących wyższe profile ryzyka stopy procentowej i płynności. Rezerwa Federalna monitoruje również „potencjalne pogorszenie jakości kredytów” w segmentach CRE i kredytów konsumenckich. W szczególności władze amerykańskie bardzo uważnie monitorują ryzyko wynikające z rynku CRE (jak ryzyko koncentracji, ekspozycje na ryzyko i zarządzanie ryzykiem) akcentując znaczenie odpowiednich buforów kapitałowych, zdolnych do absorbcji potencjalnych strat.

Przeprowadzona analiza dokumentuje także słabości, jakie utrzymują się w ‘słabym ogonie’ banków. Oprócz niezrealizowanych strat wynikających ze zmiany stóp procentowych amerykański sektor bankowy boryka się również z wyższym ryzykiem kredytowym z ekspozycji CRE i wyzwań strukturalnych spowodowanych pan-

[17] https://www.imf.org/en/Publications/WP/Issues/2023/09/06/Good-Supervision-Lessons-from-the-Field-538611 + https://www.imf.org/en/Blogs/Articles/2023/09/18/financial-stability-needs-supervisors-with-the-ability-and-will-to-act

demią. Ponadto wyzwaniem dla sektora CRE są trudne warunki rynkowe, a także rosnąca liczba przypadków niewypłacalności[18].

Jeśli stabilność finansowa jest zagrożona, utrzymanie zaufania ma kluczowe znaczenie. Jak podkreślono w raporcie na temat globalnej stabilności finansowej z kwietnia 2023 r., decydenci powinni działać szybko i zapewnić wsparcie płynnościowe, aby zapobiec zdarzeniom systemowym, które mogłyby osłabić odporność globalnego systemu finansowego. Pod tym względem odważne i szybkie działania podjęte przez władze USA pozwoliły powstrzymać bezpośrednie zagrożenie dla stabilności finansowej.

[18] Federal Reserve, Supervision and Regulation Report, November 2023. Supervision and Regulation Report, November 2023 (federalreserve.gov)

DOI: 10.26354/bb.2.1.94.2024

Patryk Król*
ORCID: 0000-0003-4079-8849
patkro12@gmail.com

Phishing jako zagrożenie dla bezpieczeństwa bankowości cyfrowej

Streszczenie

Przedmiot i cel pracy: Celem niniejszego artykułu jest analiza zagrożenia phishingiem, jako głównego wyzwania dla bezpieczeństwa bankowości cyfrowej. Praca skupia się na identyfikacji metod ataków phishingowych, ocenie skuteczności działań obronnych podejmowanych przez instytucje finansowe oraz proponuje rozwiązania mające na celu zminimalizowanie ryzyka dla klientów.

Materiały i metody: Analiza oparta jest na badaniach przeprowadzonych przez różne instytucje, w tym CERT Polska, oraz na analizie konkretnych przypadków ataków phishingowych udokumentowanych przez te organizacje. Zostały wykorzystane również dane statystyczne dotyczące świadomości społeczeństwa w zakresie zagrożeń phishingiem. Metody badawcze obejmują również studium przypadków ataków, analizę przykładów fałszywych stron bankowych oraz propozycje działań prewencyjnych.

Wyniki: Analiza wykazała, że phishing nadal stanowi istotne zagrożenie dla sektora bankowego, a ataki tego rodzaju są często skierowane na klientów instytucji finansowych. Badania pokazują, że mimo działań obronnych podejmowanych przez banki, skuteczność ataków phishingowych utrzymuje się, co wskazuje na potrzebę ciągłego doskonalenia strategii bezpieczeństwa.

Wnioski: Praca sugeruje, że banki powinny kontynuować edukację swoich klientów w zakresie rozpoznawania zagrożeń phishingowych. Ponadto, wprowadzenie dodatkowych metod autoryzacji, jak klucze U2F, może stanowić skuteczną ochronę przed atakami. Warto również zwrócić uwagę na grupy bardziej narażone na ataki phishingowe, takie jak osoby starsze, i dostosować działania edukacyjne do ich potrzeb. Praca wskazuje na konieczność ciągłego dostosowywania strategii bezpieczeństwa banków do ewoluującego krajobrazu cyberbezpieczeństwa.

Słowa kluczowe: pishing, spear pishing, whaling, smishing, vishing, calendar pishing, pharming

Kody JEL: L86

* Patryk Król – Uniwersytet Ekonomiczny w Poznaniu, Katedra Pieniądza i Bankowości.

Phishing as the main threat to digital banking security

Abstract

Subject and purpose of the work: The aim of this article is to analyze the threat of phishing as the main challenge to the security of digital banking. The work focuses on identifying methods of phishing attacks, assessing the effectiveness of defensive actions taken by financial institutions, and proposes solutions to minimize the risk for customers.

Materials and methods: The analysis is based on research conducted by various institutions, including CERT Polska, and on the analysis of specific cases of phishing attacks documented by these organizations. Statistical data on public awareness of phishing threats was also used. Research methods also include case studies of attacks, analysis of examples of fake banking websites and proposals for preventive actions.

Results: The analysis showed that phishing still poses a significant threat to the banking sector, and attacks of this type are often directed at customers of financial institutions. Research shows that despite defensive actions taken by banks, the effectiveness of phishing attacks remains, which indicates the need to constantly improve security strategies.

Conclusions: The work suggests that banks should continue to educate their customers in recognizing phishing threats. Moreover, introducing additional authorization methods, such as U2F keys, can provide effective protection against attacks. It is also worth paying attention to groups that are more vulnerable to phishing attacks, such as the elderly, and adapting educational activities to their needs. The work indicates the need to constantly adapt banks' security strategies to the evolving cybersecurity landscape.

Keywords: pishing, spear pishing, whaling, smishing, vishing, calendar pishing, pharming

JEL Codes: L86

Wstęp

Phishing to popularna metoda oszustwa, polegająca na podszyciu się pod zaufaną osobę lub instytucję w celu wyłudzenia poufnych danych, zainstalowaniu szkodliwego oprogramowania lub nakłonienia phishingowanego podmiotu do wykonania czynności, na której zależy oszustowi (por. Bieńkowska i Falkowski-Gilski 2021). Metoda ta różni się od typowego ataku hakerskiego, w którym cyberprzestępca łamie hasła zabezpieczające dostęp do rachunku bankowego, po czym włamuje się na konto, aby dysponować środkami właściciela, bądź wyrządzić określoną szkodę. Atrakcyjność phishingu dla przestępców wynika z możliwości obejścia zabezpieczeń chroniących rachunki klientów banków, pomimo tego, że w wielu nowoczesnych usługach zabezpieczenia są trudne albo z założenia niemożliwe do złamania

Według Xopero (2021) phishing znalazł się na drugim miejscu wśród zagrożeń w deklaracjach polskich firm (39,8% wskazań po ransomware – 78,2%). Natomiast według KPMG (2024) phishing jest uważany przez większość firm za największe ryzyko cybernetyczne, podobnie jak w ich wcześniejszych badaniach. Z badania SMSAPI (2024) wynika, że phishing jest również dużym zagrożeniem dla klientów;

53,7% respondentów zadeklarowało, iż otrzymało podejrzane treści, a 17,8% iż padło ofiarą oszustwa internetowego. Jak zauważa Ciulkin-Sarnocińska (2015), najczęstszym celem phisherów są banki oraz aukcje internetowe, z kolei najczęstszymi metodami jest rozsyłanie wiadomości e-mail podszywających się pod oficjalne komunikaty banków, zwykle z prośbą o zmianę hasła, odwołanie wysoko wartościowej płatności etc. Często komunikaty te zawierają błędy, z których do najczęstszych należą proste błędy ortograficzne i składniowe. Dzięki temu ofiara może już na początku oszustwa rozpoznać prawdziwego nadawcę wiadomości. Maile phishingowe są zwykle wysyłane z adresów podszywających się pod prawdziwą instytucję[1].

Banki przeciwdziałają phishingowi głównie w sposób defensywny,. poprzez informowanie użytkowników o zagrożeniach, w komunikatach lub na stronach logowania do bankowości elektronicznej (np. PKO BP, Pekao, ING, Santander, VeloBank, Millenium, grupa SGB oraz Bank Spółdzielczy w Brodnicy i Krakowski Bank Spółdzielczy). Działania informacyjne na stronach logowania podejmują również inne instytucje finansowe, jak spółdzielcze kasy oszczędnościowo-kredytowe korzystające z systemu eSKOK. Natomiast w niektórych bankach nie ma takich komunikatów na stronie głównej, gdyż odpowiednie informacje wymagają skorzystania ze specjalnego linku. Te ostatnie rozwiązania są niebezpieczne zwłaszcza dla osób mniej obeznanych z techniką korzystania z bankowości elektronicznej.

Rozwój cyberprzestępczości jest co najmniej paralelny do rozwoju bankowości internetowej. W przypadku cyberataków Krzysztoszek (2017) rozróżnia ataki na infrastrukturę bankową oraz na infrastrukturę klientów. Kluczowe jest zatem, aby w przypadku ataków, których obiektem jest klient banku, miał on odpowiednią wiedzę i narzędzia, aby się przed nimi uchronić. Rabka (2020) pisze, że osoby 65+ stanowią szczególną grupę ryzyka w kontekście zagrożeń z Internetu, co powinno skłaniać instytucje finansowe do należytej troski o ich właściwe informowanie.

Ostatnio ważne działanie z zakresu profilaktyki i zapobiegania cyberprzestępczości podjęło Biuro Informacji Kredytowej dla swych klientów korzystających z usługi „Alerty BIK". W celu lepszej ochrony klientów BIG przed oszustwami i wyłudzeniami 15 kwietnia 2024 r. uruchomiono nową usługę „ostrzeżenia BIK" w formie mailowych powiadomień o różnych niebezpiecznych zjawiskach w cyberprzestrzeni (np. masowych wyciekach danych, metodach kradzieży danych i pieniędzy stosowanych przez oszustów) oraz podejrzanych firmach działających na rynku finansowym. Oprócz informacji o zagrożeniu wysyłane będą również porady, co należy zrobić w danej sytuacji, nawet jeżeli te zdarzenia nie dotyczą bezpośrednio danego klienta, ale warto, aby wiedział i mógł prawidłowo zareagować na nie. Dodatkową korzyścią jest możliwość udostępniania tych informacji znajomym[2].

[1] Przykłady fałszywych witryn, komunikatów oraz wiadomości kierowanych do ofiar zostaną omówione w osobnym rozdziale.

[2] Regulamin Promocji Ostrzeżenia BIK. www.BIK.pl (dostęp 11.04.2024).

1. Metody ataków phishingowych

Podstawowy atak phishingowy polega na zastosowaniu socjotechnik w celu zmanipulowania ofiary, aby ta przekazała przestępcom potrzebne im dane wrażliwe (Matacz i Vodičková 2023). Choć finalnym celem ataku phishingowego jest najczęściej wyłudzenie pieniędzy, może mieć on również na celu pozyskanie informacji wrażliwych, bądź zainstalowanie złośliwego oprogramowania umożliwiającego następne ataki.

Zasadniczo phishing dzieli się według sposobu przeprowadzenia ataku oraz atakowanego podmiotu.

Ze względu na metodę przeprowadzenia ataku phishing można wyróżnić przede wszystkim:

1) Smishing (SMS phishing) – polega na wykorzystaniu spreparowanych wiadomości SMS (Yeboah-Boateng i Amanor 2014) z użyciem techniki *spoofingu*, której efektem jest wyświetlenie fałszywej nazwy (ID) nadawcy, w celu podszycia się pod określoną osobę, bądź instytucję (Piotrowski i Różanowski 2012).
2) Vishing – polega na telefonicznym wyłudzeniu danych wrażliwych (Laszczak 2019), niekiedy także z wykorzystaniem techniki *spoofingu* (Piotrowski i Różanowski 2012).
3) Quishing – polega na umieszczeniu w kodzie QR zainfekowanego adresu URL (Sharevski, Devine, Pieroni i Jachim 2022), przekierowującego ofiarę do spreparowanej strony wiarygodnej dla niego instytucji (np. finansowej), bądź do strony pobierania zawirusowanego pliku.
4) Calendar phishing – polega na nakłonieniu ofiary do dodania zainfekowanego kalendarza w odpowiedniej aplikacji (np. kalendarz Google). Cyberprzestępcy mogą za pośrednictwem własnego kalendarza wysyłać zaproszenia do zainfekowanych stron (Alghenaim, Bakar i Rahim 2022). Sprzyja temu ustawienie automatycznej akceptacji zaproszeń do kalendarzy, które w niektórych aplikacjach są domyślne.
5) Page hijacking – polega na przekierowaniu użytkownika do spreparowanej przez przestępców zainfekowanej strony, lub strony do której cyberprzestępcy wcześniej się włamali (Thakur i Verma 2014).
6) Pharming – polega najczęściej na podmianie pliku *hosts* (Singh 2011) tłumaczącego nazwy domen DNS na IP. Mimo że użytkownik wpisuje poprawną nazwę domeny (np. pkobp.pl) zostaje przekierowany do domeny o innym adresie IP, ale podobnym lub identycznym wyglądzie strony (Kim, Kang i Kim 2015).
7) AIshing – użycie sztucznej inteligencji, technologii uczenia maszynowego lub zaawansowanych modeli językowych zaczyna być coraz bardziej popularne także wśród cyberprzestępców. W nieodległej przyszłości może być to jedna z najpopularniejszych oraz najtrudniejszych do rozpoznania metod ataków phishingowych.

Ze względu na adresata ataku phishingowego można wyodrębnić dwa rodzaje:

1) *Spear phishing* – to spersonalizowany atak phishingowy (Xu, Singh i Rajivan 2023) polegający na starannie spreparowanych wiadomościach (mogących przybierać zarówno formę e-mail, SMS, połączeń telefonicznych, alertów i innych) zawierających informacje dedykowane specyficznie dla danych osób i organizacji będących celem ataku (Schuetz, Lowry i Thatcher 2016).
2) Whaling (CEO fraud) – to atak podobny do ataku *spear phishing*, ukierunkowany na ważnych pracowników (dyrektorów generalnych, dyrektorów finansowych etc.) oraz zamożnych klientów (Kalaharsha i Mehtre 2021). Atak ten można uznać jako szczególny typ ataku *spear phishing*.

Ze względu na pewne typowe cechy w phishingu wyróżnia się zasadniczo cztery fazy działalności przestępcy (Bieńkowska i Falkowski-Gilski 2021 oraz Alkhalil, Hewage, Nawaf i Khan 2021):

1) Faza planowania – cyberprzestępca zbiera informacje o potencjalnych ofiarach, wybiera cel oraz metodę ataku.
2) Faza przygotowania – cyberprzestępca wyszukuje luki oraz słabe punkty w architekturze cyberbezpieczeństwa atakowanego podmiotu, a także wybiera najbardziej dopasowany środek przekazu.
3) Faza ataku – dochodzi do interakcji cyberprzestępcy z ofiarą lub grupą ofiar w celu skłonienia ich do wykonania pożądanej przez cyberprzestępcę czynności. Atak najczęściej zaczyna się od wiadomości, która ma na celu skłonić ofiarę do kliknięcia w link podobny do oryginalnego.
4) Faza wykorzystania informacji – dochodzi do wykorzystania udzielonych przez ofiarę informacji, lub wytworzonych przez nią luk w zabezpieczeniach systemu (tzw. *backdoor*).

2. Przykłady ataków phishingowych

Warto podkreślić, że metody ataków phishingowych pozostają dość podobne, jednak są systematycznie udoskonalane. W tej części artykułu scharakteryzowano przykłady ataków phishingowych przeprowadzone przez oszustów, jakie zostały udokumentowane przez Zespół Reagowania na Incydenty Bezpieczeństwa (ang. akronim CERT) działający w NASK (Naukowa i Akademicka Sieć Komputerowa) stronę www:niebezpiecznik.pl, zajmującą się zarówno popularyzowaniem wiedzy, jak i szkoleniami z zakresu cyberbezpieczeństwa.

Tabela 1. Linki oryginalnych oraz fałszywych stron bankowych

Link oryginalny	Link fałszywy
https:// ipko.pl	https://iko-pl.pw (niebezpiecznik.pl 2023a)
	https://ipko-zablokowany.net (niebezpiecznik.pl 2023b)
	http://www.ipko.co/ (Konieczny 2014)
	http://www.pkobp-online.com/ (Konieczny 2014)
	http://online-pkobp.net/ (Konieczny 2014)
	http://www.myipko.net/ (Konieczny 2014)
	www.weryfikacja-ipko.cu.cc (niebezpiecznik.pl 2013)
BLIK nie ma oficjalnej strony przeznaczonej do płatności, opiera się na systemach płatności online, jak Przelewy24, PayU czy TPay.	https://link.sv/blik (Konieczny 2022)
https://login.ingbank.pl/mojeing/app/	https://login-ingbank.pl-id891uah1zvav18zbga81b.com (niebezpiecznik.pl 2022a)
https://online.mbank.pl/pl/Login	https://s3.amazonaws.com/sledeniepoljak/2/pl.html (niebezpiecznik.pl 2022b) https://rondo.su/mbanku-poland/ (niebezpiecznik.pl 2022b)

Źródło: opracowanie własne, na podstawie serwisu niebezpiecznik.pl

Fałszywy link zwykle nawiązuje lub jest podobny do oryginalnego, jednak znacznie różni się od oryginalnego. Często fałszywy link wykorzystuje protokół HTTPS, który często nadal błędnie jest uważany za gwarancję bezpieczeństwa. Jak zauważa Guga (2007) zadaniem protokołu HTTPS jest ochrona danych przed przechwyceniem przez osoby niepowołane, jednak hasło użytkownika w protokole HTTP wysyłane jest w sposób jawny, co pozwala na odczytanie go przez osoby niebędące adresatami. Cyberprzestępca, jako właściciel domeny i adresat, zgodnie z działaniem protokołu HTTPS może odczytać przesłane mu hasło.

Kolejnym elementem w przestępczym procesie naruszania cyberbezpieczeństwa jest domena do jakiej prowadzą fałszywe linki. Przykładem tego są domeny należące do Palau (.pw), Wysp Kokosowych (.cc), Kolumbii (.co), Salwadoru (.sv), ale również domen międzynarodowych (.com, .net). Oznacza to, że phishing ma międzynarodowy i masowy charakter (Jancelewicz 2022), a przestępcy liczą, że w dużym zbiorze adresatów wiadomości zaledwie niewielki procent zareaguje zgodnie z ich intencją. Według raportu CERT (2023c) najpopularniejszą domeną wykorzystywaną przez cyberprzestępców była domena: .com (6690 przypadków, tj. 41,59% zgłaszanych domen), .pl (3375 przypadków), .online (592 przypadki), .net (509 przy-

padków), .dev (485 przypadków), .info (435 przypadków), .eu (425 przypadków), .org (416 przypadków), .cfd (397 przypadków), .site (342 przypadki). Według CERT korzystanie z domen .com i .pl wynika najprawdopodobniej z ich popularności, a także stereotypowego zaufania użytkowników. Ma to negatywny wpływ na cyberbezpieczeństwo i rzutuje na skuteczność działań przestępców. Z kolei popularność takich domen, jak np. .xyz, wynika z ich niższej ceny i większej dostępności nazw.

Według informacji niebezpiecznik.pl (2014) tylko w jednym ataku przeciw klientom PKO BP przestępcy próbowali wygenerować ok. 100 transakcji, na średnią kwotę 3000 zł, z czego, niestety, kilkanaście przestępczych transferów było udanych. Wykradzione w ten sposób środki zasilały karty *pre-paid* dzięki którym przestępcy mogli wypłacać pieniądze. W początkowych fazach wyłudzenia danych przestępcy posługiwali się własną stroną, tj. oknem logowania, oraz oknem, w którym proszono o podanie dziesięciu kodów z karty kodów jednorazowych (niebezpiecznik.pl 2013). Po udanej akcji uzyskania kodów przekierowywano ofiarę na prawdziwy adres banku, co tłumaczono koniecznością ponownego zalogowania.

Jak zauważa SMSAPI (2024) najłatwiejszymi do zidentyfikowania dla klientów elementami fałszywej wiadomości są:

- ponaglenie do działania zawarte w wiadomości, zwykle z podanym krótkim czasem na reakcję odbiorcy (65,2%),
- nieznany numer, adres lub nazwa nadawcy wiadomości (61,6%),
- zamieszczenie linku (60%),
- brak kontekstu wiadomości,
- niespodziewana wiadomość (58,7%),
- błędy składniowe, ortograficzne, typograficzne (58,6%),
- załączony nietypowy, dziwny adres WWW (58,3%),
- straszenie odbiorcy konsekwencjami (50,2%),
- brak odniesienia do danych odbiorcy (50,2%).

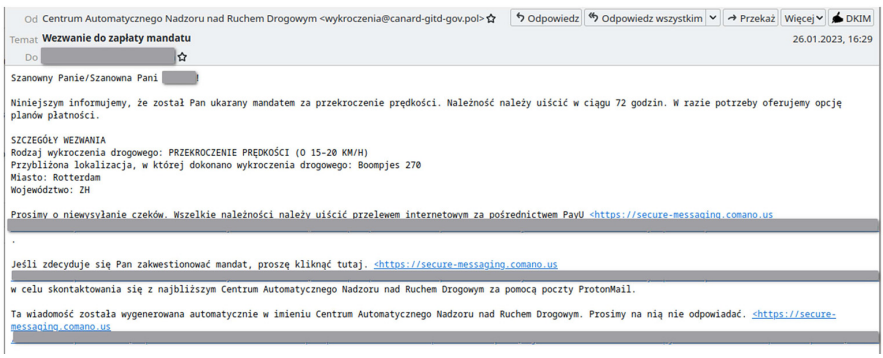
Powyższe cechy wiadomości odnoszą się głównie do podstawowej, masowej formy phishingu. W dobie powstawania coraz bardziej rozbudowanych modeli językowych (np. GPT 4.0, GPT 5.0), z których część dostępna jest bezpłatnie, tworzenie wiarygodnych wiadomości eliminujących te podejrzane staje coraz łatwiejsze. Dlatego profilaktyka, prewencja i zapobieganie oszustwom phishingowym powinny uwzględniać nie tylko te znane, ale także te potencjalne formy phishingu uwzględniające zastosowanie zaawansowanych modeli językowych, nagrań obrazu i głosu wygenerowanych przy użyciu uczenia maszynowego itp. Tym bardziej, że w zasadzie bez ograniczeń dostępne są narzędzia pozwalającego spreparować nagranie z wizerunkiem lub głosem danej osoby. Mają jednak jeszcze stosunkowo łatwo identyfikowane wady (np. charakterystyczna chrypa wygenerowanego głosu, zniekształcenia obrazu przy dynamice postaci, ręki przykładanej do wygenerowanej komputerowo twarzy). Niestety, są już także dostępne bardziej zaawansowane technologicznie narzędzia, dające wyższą jakość generowanego materiału o wyższych kosztach nabycie. Obecnie media publikują już przypadki oszustw z wykorzystaniem sklonowanego głosu (Stefanicki 2023).

Rysunek 1. Post oszustów podszywających się pod Bank Pekao w serwisie Facebook

Źródło: CERT Polska, 2022.

Łatwo zidentyfikować, że w opisach występują czcionki typowe dla cyrylicy, które wkomponowano w treść edytowaną w czcionkach łacińskich. Zabieg ten miał na celu uniknięcie automatycznego wykrycia przez administrację portalu banku. Warto dodać, że domena .icu, która została użyta w tym ataku należy do prywatnej chińskiej firmy Alibaba.

Rysunek 2. Przykład maila phishingowego

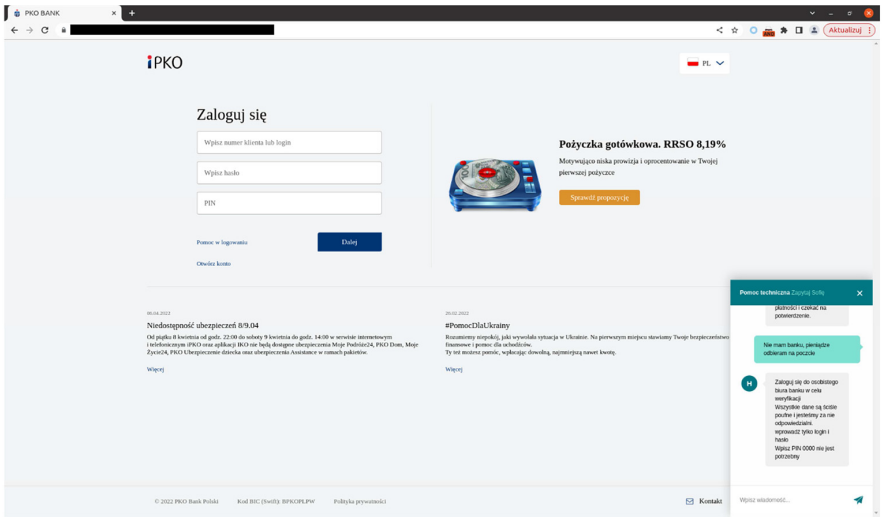


Źródło: CERT Polska, 2023a

Treść maila z rysunku 2 jest przykładem masowego phishingu. Mail jest w wielu miejscach niedopracowany, potencjalna ofiara może zidentyfikować go m.in. po dziwnym adresie e-mail nadawcy, podejrzanych linkach, ponagleniu do wykonania transakcji oraz nieistniejącej instytucji, pod jaką podszywa się nadawca. Ponadto, mail odnosi się do rzekomego wykroczenia drogowego popełnionego w Rotterda-

mie „w województwie ZH", podział administracyjny Królestwa Niderlandów opiera się jednak na prowincjach. Prawdopodobnie wiadomość była szablonem skierowanym do wielu odbiorców w różnych krajach, a odniesienie się w treści do holenderskiego województwa było próbą dostosowania wiadomości do polskiego odbiorcy, zarazem próbą uwierzytelnienia maila w oczach ofiary poprzez zawarcie szczegółowych danych.

Rysunek 3. Przykład fałszywej strony logowania



Źródło: CERT Polska 2023b.

Na fałszywej stronie internetowej banku (rys. 3) widoczny jest przede wszystkim niepasujący graficznie element czatu z „pomocą techniczną". Adresat napisał (dolny prawy prostokąt), że nie ma konta w banku, a pieniądze odbiera na poczcie, a najprawdopodobniej otrzymał automatyczną odpowiedź z poleceniem zalogowania, zapewnieniem o poufności i „odpowiedzialności o dane" banku, oraz informację, że podanie numeru PIN nie jest konieczne. Uważni klienci wiedzieli, że bank PKO BP nie wymagał w pierwszym kroku do logowania w bankowości internetowej numeru PIN, ponadto konieczne do zalogowania hasło pojawiało się dopiero w następnym kroku i na oddzielnej stronie wraz z wybranym przez klienta obrazkiem, stanowiącym jedno z zabezpieczeń przed wyłudzeniem danych.

3. Poziom zagrożenia phishingem w sektorze bankowym w Polsce

Badania Piłata, Pawłowskiego i Kozieła (2022) wskazują, że 77% Polaków nie wie, czym jest phishing. Natomiast największą znajomość phishingu wykazali respondenci w grupie wiekowej 20–24 lata (43%) Autorzy prezentują także reakcje respondentów na prośbę o ocenę, czy przedstawiony im przykład wiadomości mailowej jest wiadomością o charakterze phishingowym. Tylko 27% respondentów odpowiedziało poprawnie, 68% respondentów nie potrafiło udzielić poprawnej odpowiedzi, a 5% zareagowało błędnie. Niski stan świadomości o zagrożeniach atakiem phishingowym potwierdza raport SMSAPI (2024), z badania polegającego na rozpoznaniu oryginalności komunikatu. 30% respondentów wskazało wszystkie trzy fałszywe komunikaty, 47% wskazało wszystkie wiadomości jako fałszywe, 53% wskazało prawdziwą wiadomość jako fałszywą. Jednocześnie aż 62 badanych zadeklarowało, że potrafi rozpoznać fałszywy komunikat. Scharakteryzowane wyniki badań uświadamiają konieczność intensywnej edukacji klientów w zagadnieniach cyberbezpieczeństwa, gdyż w przypadku ataku phishingowego to klient banku stanowi najsłabsze ogniwo łańcucha bezpieczeństwa.

W 2022 r. CERT Polska (2023c) zarejestrował 25 625 incydentów o charakterze phishingu, co stanowiło 64% wśród wszystkich obsłużonych przez CERT incydentów. Przy czym najczęściej wykorzystywana była marka InPost (5119 incydentów), Facebook (4370 incydentów) oraz Vinted (2926 incydentów). Również Zespół CSIRT KNF realizujący zadania Sektorowego Zespołu Cyberbezpieczeństwa, we współpracy z podmiotami krajowego systemu cyberbezpieczeństwa, a w szczególności zespołami CSIRT poziomu krajowego, wspiera Operatorów Usług Kluczowych w obsłudze poważnych incydentów występujących w tych podmiotach, a także prowadzi działania mające na celu analizę pozostałych incydentów, trendów i zagrożeń w obszarze cyberbezpieczeństwa. Instytucja ta (CSIRT KNF 2023) potwierdza, że phishing jest najczęściej stosowaną metodą kradzieży środków finansowych.

3.1. Główne metody zapobiegania phishingowi

Masowość i kreatywność cyberprzestępców wymaga przeciwdziałania ich zamierzeniom czy działaniom na wszystkich fazach phishingu. Utrudnienie planowania phishingu wymaga ograniczenia dostępu do danych wrażliwych, w tym także dotyczących codziennego życia prywatnego klientów. Chodzi o to, aby cyberprzestępca miał jak najmniejszą szansę na uwierzytelnienie siebie dzięki znajomości informacji o potencjalnej ofierze ataku (np. różne próbki głosu służące do wygenerowania potrzebnego komunikatu). Przeciwdziałając intencjom przestępcy w fazie przygotowania ataku, potrzebne jest minimalizowanie luk bezpieczeństwa, zarówno luk oprogramowania, jak i sprzętowych. Służą temu terminowe aktualizacje czy zapory sieciowe (*firewall*). W fazie ataku cyberprzestępca nawiązuje pośredni lub bezpośredni kontakt z ofiarą, co wymaga z jej strony zachowania ostrożności wynikającej m.in. z posiadanej wiedzy

o zagrożeniach. Przede wszystkim minimalizowanie dostępu do informacji o ofierze, a także gotowość i umiejętność zweryfikowania wiedzy przestępcy na swój temat. W ostatniej fazie kluczowa jest rola instytucji finansowych w doskonaleniu identyfikacji prawdziwości danych (w tym kody autoryzacyjne) w trakcie ataku. Przy czym trzeba pamiętać, że w świetle przepisów prawa udostępnienie takich danych komukolwiek kto nie jest właścicielem rachunku bankowego wyłącza odpowiedzialność instytucji finansowych (Popik i Gryglicka 2022).

Niemniej ważne jest również budowanie przez banki, wspólnie z instytucjami sieci bezpieczeństwa finansowego oraz okołobankowymi kultury cyberbezpieczeństwa. Można nawet spotkać opinie, że kultura cyberbezpieczeństwa może w przyszłości stać się nadrzędnym zbiorem wartości wobec wszelkich innych norm dotyczących bezpieczeństwa państwa i obywateli (Górka 2018). Zidentyfikowane trendy zagrożeń cyberbezpieczeństwa wymagają skoordynowanej działalności szkół wszystkich szczebli, a uwzględniając koncepcję uczenia się przez całe życie (ang. *long life learning*) także tzw. edukacji trzeciego wieku. Przykładem działań w tym zakresie podejmowanych przez sektor bankowy jest m.in. projekt „Bezpieczeństwo w Cyberprzestrzeni" realizowany przez Warszawski Instytut Bankowości wraz z partnerami (Visa, Santander, Fundacja Polska Bezgotówkowa, mBank, Allegro oraz Bank Pekao). Warto zwrócić uwagę, że jednym z podmiotów jest firma Allegro, która nie jest częścią sektora finansowego. Może to wynikać z faktu, że wiele ataków phishingowych nakierowanych jest na klientów Allegro. Projekt jest kierowany głównie do studentów (95 tysięcy uczestników) oraz seniorów (8 tysięcy uczestników) (ZBP 2022). Działania na rzecz edukacji w obszarze cyberbezpieczeństwa podejmuje również CSIRT KNF, a są one adresowane głównie do sektora finansowego (CSIRT KNF 2023). Cyberbezpieczeństwo może być też jednym z obszarów międzypokoleniowego uczenia się, jak zauważa Rojek (2019) potencjał uczenia międzypokoleniowego w zakresie cyberprzestrzeni jest duży, lecz nie jest w pełni wykorzystany. Dalej wywodzi on, że międzypokoleniowe uczenie należy animować, wspierać i stwarzać korzystne dla niego warunki wykorzystując narzędzia ICT (technologie informatyczno-komunikacyjne). Oleksiewicz (2019) natomiast eksponuje ważną rolę w kształtowaniu obywatelskiej kultury bezpieczeństwa, m.in. poprzez samokształcenie w zakresie bezpieczeństwa w sieci.

Ponadnarodowy charakter z perspektywy legislacyjnej jest ważnym wydarzeniem dla zwiększania poziomu cyberbezpieczeństwa, dowodzi uchwalenie i wdrożenie dyrektywy PSD2. Przepisy dyrektywy mają na celu wprowadzenie wyższego poziomu bezpieczeństwa podczas przeprowadzania transakcji oraz umożliwienie powstawania innowacji płatniczych; wyrażają również obawy co do możliwego spadku liczby transakcji ze względu na wprowadzone zabezpieczenia (Grzywacz i Jagodzińska-Komar 2018). Jagodzińska-Komar (2016) zauważa również, że na dostawców usług płatniczych został nałożony obowiązek silnego uwierzytelniania klientów (SCA), metoda ta wymaga użycia specjalnych urządzeń cyfrowych (token, karta elektroniczna) lub mechanizmów cyfrowych (klucze kryptograficzne, certyfikaty cyfrowe). Metoda ta łączy się przeważnie z hasłem, dzięki czemu w przypadku kradzieży urządzenia staje się ono bezużyteczne. Silne uwierzytelnianie – w myśl

dyrektywy PSD II – wymaga dwóch, spośród trzech, elementów weryfikujących klienta (np. hasło, kod PIN), posiadanie (np. telefonu komórkowego), cechy klienta (np. cechy biometryczne) (Gradzi 2017). Z obowiązku silnego uwierzytelniania Europejski Urząd Nadzoru Bankowego zwolnił płatności niskokwotowe. Hałasik-Kozajda i Olbryś (2021) zwracają uwagę, że wdrożenie dyrektywy PSD2 w obszarze cyberbepieczeństwa może generować dotkliwe dla mniejszych instytucji finansowych koszty. Kotliński (2022) twierdzi, że jednym z rozwiązań ograniczenia kosztów, tworzenia, rozwoju i bieżącej obsługi systemów IT w bankowości spółdzielczej mogłoby być tworzenie systemów informacyjnych obejmujących cały sektor bankowości spółdzielczej, nie zaś pojedyncze banki, a nawet zrzeszenia.

Jednym z najbezpieczniejszych narzędzi autoryzacji są klucze U2F oraz hasło jednorazowe ograniczone czasowo (OTP). Algorytmy OTP dzielą się głównie na dwa rodzaje, HOTP (HMAC-based One-time Password), czyli algorytm w którym najważniejszą zmienną jest wygenerowane hasło, które pozostaje aktywne do czasu wysłania kolejnej prośby do serwera o wygenerowanie nowego hasła, oraz TOTP (Time-based One-time Password), w którym po określonym, z góry ustalonym czasie staje się nieważne (Digital Fingerprints 2022). Obecnie jedno z narzędzi autoryzacji korzystającym z TOTP, jakim jest token, jest w praktyce dla klientów indywidualnych niedostępny, ze względu na wymóg podania klientowi przed zaakceptowaniem transakcji informacji o jej kwocie i odbiorcy (Samcik 2019). Większość dotychczas stosowanych tokenów (tokeny RSA) była zdolna wyświetlić jedynie kod autoryzacyjny. Część banków (np. Millenium, Credit Agricole) oferuje obecnie tokeny sprzętowe nowego typu, oparte na technologii Cronto (Zagańczyk 2019), która wykorzystuje podobne graficznie do kodów QR graficzne kryptogramy, składające się z matrycy kolorowych kropek, wyświetlanych na ekranie komputera, które następnie można zeskanować tokenem sprzętowym. Bank Credit Agricole oferuje token sprzętowy zarówno dla firm, jak i klientów indywidualnych, zgodnie z tabelą opłat w zależności od typu konta korzystanie z tokena może być bezpłatne, lub obarczone opłatą 7 zł lub 9 zł (Credit Agricole 2024). W przypadku banku Millenium token sprzętowy jest dedykowany dla klientów bankowości przedsiębiorstw, a korzystanie z niego jest obarczone jednorazową opłatą 200 zł za wydanie urządzenia (bankmillenium.pl n.d.). Niska dostępność tokenu może wynikać głównie z ich kosztu, konieczności wymiany baterii, a także skomplikowanie urządzenia i częste gubienie ich przez klientów (niebiezpiecznik.pl 2018). Klucz U2F jest kluczem sprzętowym podobnym do nośnika typu pendrive, najczęściej z wyjściem USB, mikro-USB, lub USB typu C. W standardzie protokołu U2F mogą działać również klucze w technologii Bluetooth oraz NFC (Srinivas, Balfanz, Tiffany i Czeskis 2015). Główną wadą kluczy U2F jest konieczność ich zakupu oraz konieczność posiadania urządzenia w celu autoryzacji logowania do innych urządzeń. Klucze te są powszechnie uważane za jeden z najlepszych narzędzi uwierzytelniania logowania (niebezpiecznik.pl 2021). Chociaż wygodniejszym i łatwiejszym do publicznego użytku rozwiązaniem są aplikacje obsługujące algorytmy TOTP, jak np. Google Authenticator, Microsoft Authenticator czy KeePassXc.

4. Propozycje działań banków

Analizy aktywności cyberprzestępców z wykorzystaniem phishingu wskazują, że nadal bazować będą na masowych atakach. Jednakże elastyczność reakcji świata przestępczego nie wyklucza zmiany taktyki i posługiwanie się zaawansowanymi technikami generowania komunikatów o wyższym stopniu wiarygodności dla ofiar poprzez wykorzystywanie indywidualnie dedykowanych przekazów, skierowanych tylko do celowo wybranych osób. W literaturze taką taktykę ataku określa się jako *spear phishing* (Pitera 2017). Biorąc pod uwagę analizę kosztów i efektów, można założyć, że nadal jeszcze wariant masowych ataków będzie dominował dopóki będzie on bardziej dochodowy.

Urząd Komisji Nadzoru Finansowego (UKNF) zaleca wdrożenie uwierzytelniania wieloskładnikowego tożsamości klienta w elektronicznych kanałach dostępu (Pisarewicz i Podlewski 2023). Propozycja ta, mimo że zmniejsza prawdopodobieństwo udanego ataku hakerskiego, nie eliminuje całkowicie problemu ataków phishingowych, ponieważ w takich sytuacjach to użytkownik ujawnia różnorodne kody autoryzacyjne osobom nieuprawnionym.

Stosunkowo dobrą praktyką w zakresie przeciwdziałania phishingowi jest możliwość weryfikacji danego pracownika lub połączenia telefonicznego na oficjalnej stronie banku lub w aplikacji banku. Takie rozwiązanie obecnie ma w swojej ofercie PKO BP (pkobp.pl 2022) oraz mBank (mbank.pl 2023), polega ono na przekazaniu klientowi danych pracownika w oficjalnej aplikacji danego banku oraz wymogu zatwierdzenia rozmowy telefonicznej z doradcą. W ten sposób potwierdzana jest również tożsamość klienta, dzięki czemu możliwa do uniknięcia jest mało wygodna metoda autoryzacji polegająca na przekazaniu ustnie numeru PESEL, nazwiska panieńskiego matki lub innych danych wymaganych do autoryzacji.

Bardziej zaawansowanym rozwiązaniem w zakresie ochrony przez phishingiem jest stosowanie kluczy U2F. Warto rozważyć odpowiednią akcję promocyjną i udostępnianie ich klientom na przykład w ramach promocji przy założeniu rachunku bankowego lub dla stałych klientów. Aktualnie koszty podstawowej wersji takiego klucza wynoszą od 150 do 200 zł, a bardziej zaawansowane egzemplarze mogą kosztować do 500 zł. Podstawowa wersja klucza U2F może być atrakcyjnym gadżetem reklamowym, zwiększającym zarazem bezpieczeństwo środków klienta. Obok efektu reklamowego takie działanie daje wizerunek banku jako instytucji troszczącej się o klienta i zapewniającej mu bezpieczeństwo. W pierwszym okresie promocji kluczy U2F, zgodnie z koncepcją krzywej doświadczenia w marketingu, pionierzy mają szansę na uzyskanie przewagi konkurencyjnej.

Klucz U2F jest wdrażany w coraz szerszym asortymencie usług z dostępem internetowym. Prym wiodą tu usługi społecznościowe oraz komunikacyjne prowadzone przez gigantów technologicznych, jak Meta czy Alphabet. Sektor bankowy w Polsce również nie lekceważy tego sposobu zabezpieczenia. Pierwszym bankiem w Polsce, który wprowadził możliwość autoryzacji kluczem U2F, był ING Bank Śląski

(Blikowska 2023). Niestety, metoda ta nie zyskała jeszcze szerszego zastosowania, ale uwarunkowania otoczenia i specyfika działalności w sektorze finansowym niezawodnie wymuszą stosunkowo szybko odpowiednie dostosowania, i to nie tylko w segmencie banków.

Dobrą praktyką w zakresie przeciwdziałania phishingowi jest możliwość weryfikacji danego pracownika lub połączenia telefonicznego na oficjalnej stronie banku lub w aplikacji banku. Takie rozwiązanie obecnie ma w swojej ofercie PKO BP (pkobp.pl 2022) oraz mBank (mbank.pl 2023), polega ono na przekazaniu klientowi danych pracownika w oficjalnej aplikacji danego banku oraz wymogu zatwierdzenia rozmowy telefonicznej z doradcą. W ten sposób potwierdzana jest również tożsamość klienta, dzięki czemu możliwa do uniknięcia jest mało wygodna metoda autoryzacji polegająca na przekazaniu ustnie numeru PESEL, nazwiska panieńskiego matki lub innych danych wymaganych do autoryzacji. Wydaje się również, że bank przy podpisywaniu umowy o prowadzenie konta powinien informować klienta o podstawowych zasadach bezpieczeństwa, możliwościach autoryzacji pracownika banku, a także o wyłączeniu odpowiedzialności banku w przypadku rażącego niedbalstwa ze strony klienta. Informacja ta powinna mieć charakter rozmowy z konsultantem, aby mieć pewność, że klient zapoznał się z informacją oraz w pełni ją zrozumiał.

Podsumowanie

Analiza zagrożeń związanych z phishingiem w bankowości elektronicznej pozwala wyciągnąć kilka istotnych wniosków. Przede wszystkim phishing stanowi realne i aktualne zagrożenie, które nie tylko nie traci na znaczeniu, ale wraz z rozwojem techniki i technologii, a także popularności bankowości internetowej, kreuje nowe formy i metody ataku.

Badania dowodzą, że przestępstwa phishingowe występują głównie w sektorze bankowym, bowiem w przypadku skutecznego ataku przynoszą wysokie korzyści finansowe. Przy czym phishing e-mailowy pozostaje nadal jedną z najczęstszych form dostępu do informacji o ofierze poprzez zdobycie jej zaufania poprzedzające uzyskanie potrzebnych danych.

Banki aktywnie przeciwdziałają zagrożeniom związanym z phishingiem. Wprowadzane są środki ochronne, jak komunikaty ostrzegawcze na stronach logowania, informacje o cyberbezpieczeństwie i edukacja klientów. Korzystają w tym ze wsparcia ogniw sieci bezpieczeństwa finansowego (np. UKNF) czy instytucji okołobankowych (np. BIK, UOKiK). Jednakże wobec dynamicznych zmian, a także wykorzystywania nowinek techniki oraz technologii wykorzystywanych przez cyberprzestępców, konieczne jest ciągłe rozwijanie strategii obronnych.

Scharakteryzowane w artykule przykłady ataków phishingowych pokazują, jak złożone i kreatywne były próby wyłudzenia danych. Wprowadzenie kluczy U2F, jako dodatkowego elementu autoryzacji klienta, stanowi krok w kierunku zwiększenia

bezpieczeństwa, jednakże z badań wynika, że świadomość i edukacja klientów w zakresie rozpoznawania zagrożeń nie idzie w parze z rozwojem zagrożeń i wymaga nowych oraz skutecznych inicjatyw, które *per saldo* okażą się tańsze niż konsekwencje przestępstw cybernetycznych. Na uwagę zasługują segmenty klientów szczególnie podatnych na cyberataki, a zwłaszcza osoby o niższych kompetencjach cyfrowych.

Podniesienie poziomu ochrony dotyczy szybkiego i powszechnego wdrożenia technologii uwierzytelniania wieloskładnikowego oraz promocję kluczy U2F. Wprowadzenie tych rozwiązań nie tylko zwiększy bezpieczeństwo, ale może również zwiększyć zaufanie klientów do instytucji finansowej.

Bibliografia

Alghenaim M.F., Bakar N.A.A., Rahim F.A. (2022), *Awareness of Phishing Attacks in the Public Sector: Review Types and Technical Approaches*, [w:] *International Conference on Emerging Technologies and Intelligent Systems* (pp. 616–629). Cham: Springer International Publishing.

Alkhalil Z., Hewage C., Nawaf L., & Khan I. (2021), *Phishing attacks: A recent comprehensive study and a new anatomy*, „Frontiers in Computer Science", 3, 563060.

Bankmillennium.pl (n.d.), *Nowy wymiar uwierzytelnienia*, https://www.bankmillennium.pl/przedsiebiorstwa/bankowosc-elektroniczna/bank-w-internecie/millenet/bezpieczenstwo/token-sprzetowy-z-czytnikiem (dostęp 15.04.2024).

Bieńkowska D., Falkowski-Gilski P. (2021), *Nauka w świecie cyfrowym okiem młodego inżyniera-phishing w mediach elektronicznych*, Pismo PG.

Blikowska J. (2023), *Banki w końcu zaczynają wprowadzać klucze U2F. Hakerom będzie trudniej* – rp.pl. Rzeczpospolita, https://pieniadze.rp.pl/konta-bankowe/art39376181-banki-polskie-klucze-u2f-hakerom-bedzie-trudniej

CERT Polska (2022), *Kampanie phishingowe wykorzystujące wizerunek banków*, https://cert.pl/posts/2022/04/banki-phishing/ (dostęp 25.12.2023).

CERT Polska (2023a), *Kampanie phishingowe na serwisy pocztowe*, https://cert.pl/posts/2023/04/phishing-webmail/ (dostęp 7.04.2024).

CERT Polska (2023b), *Kampania phishingowa wykorzystująca wizerunek Ministerstwa Finansów*, https://cert.pl/posts/2023/01/phishing-govpl/ (dostęp 7.04.2024).

CERT Polska (2023c), *Raport roczny z działalności CERT Polska 2022 – „Krajobraz bezpieczeństwa polskiego internetu"*, https://cert.pl/uploads/docs/Raport_CP_2022.pdf (dostęp 7.04.2024).

Ciulkin-Sarnocińska K. (2015), *Phishing-specyficzna forma pozyskiwania danych newralgicznych*, [w:] *Współczesne oblicza bezpieczeństwa*, red. nauk. E.M. Guzik-Makaruk, E.W. Pływaczewski (pp. 113–121). Temida 2, przy współpracy i wsparciu finansowym Wydziału Prawa Uniwersytetu w Białymstoku.

Credit Agricole (2024), *Tabela opłat i prowizji kont dla osób fizycznych*, https://static.credit-agricole.pl/asset/t/o/i/toip-indywidualni-01022024_28576.pdf (15.04.2024).

CSIRT KNF (2023), *Cyberzagrożenia w sektorze finansowym*, https://cebrf.knf.gov.pl/images/Cyberzagroenia_w_sektorze_finansowym_2022.pdf (dostęp 7.04.2024).

Digital Fingerprints (2022), *OTP, TOTP i HOTP a ochrona haseł. Co oznaczają te skróty i dlaczego warto je znać?*, https://fingerprints.digital/otp-totp-i-hotp-a-ochrona-hasel/ (dostęp 8.04.2024).

Górka M. (2018), *Kultura bezpieczeństwa w kontekście znaczenia informacji jako elementu społeczno-kulturowego*, „Przegląd Politologiczny", (2).

Gradzi D. (2017), *Bezpieczeństwo płatności elektronicznych jako element cyberbezpieczeństwa państwa–przegląd regulacji prawnych*, „Przegląd Bezpieczeństwa Wewnętrznego", 9(16).

Grzywacz J., Jagodzińska-Komar E. (2018), *Rola banków i sektora FinTech w świetle implementacji dyrektywy PSD2*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace", (2).

Guga D. (2007), *Bezpieczeństwo transakcji elektronicznych wykorzystujących infrastrukturę klucza publicznego*, „Acta Universitatis Lodziensis. Folia Oeconomica", 211.

Hałasik-Kozajda M., Olbryś M. (2021), *Skutki implementacji dyrektywy o usługach płatniczych (PSD2)*, „Bank i Kredyt", 52(3).

Iwańczuk-Kaliska A., Marszałek P., Schmidt K., Warchlewska A. (2021), *Ocena zmian na rynku płatności w Polsce*. Raport opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości (Sygn. Wib Pab 10/2021).

Jagodzińska-Komar E. (2016), *Zmiany w systemie SEPA i wpływ Dyrektywy PSD2 na rynek usług płatniczych*, „Zeszyty Naukowe PWSZ w Płocku. Nauki Ekonomiczne", 1(23).

Jancelewicz J. (2022), *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych*, „Kwartalnik Trzeci Sektor", (59–60 (3–4)).

Kalaharsha P., Mehtre B.M. (2021), Detecting Phishing Sites--An Overview. arXiv preprint arXiv:2103.12739.

Kim, S., Kang, J.Y. i Kim, Y. (2015), *Countermeasures against phishing/pharming via portal site for general users*, „The Journal of Korean Institute of Communications and Information Sciences", 40(6).

Klucz do (cyber)bezpieczeństwa – Baza wiedzy – Portal Gov.pl. (2022) Baza Wiedzy, https://www.gov.pl/web/baza-wiedzy/klucz-do-cyberbezpieczenstwa-

Konieczny P. (2014), *Uwaga klienci PKO i Citi banku! Trwa potężna kampania phishingowa, z kont skradziono już kilkanaście tysięcy złotych*, Niebezpiecznik.pl, https://niebezpiecznik.pl/post/uwaga-klienci-pko-i-citi-banku-trwa-potezna-kampania-phishingowa-z-kont-skradziono-juz-kilkanascie-tysiecy-zlotych/ (dostęp 25.12.2023).

Konieczny P. (2022), *Uwaga! Ktoś podszywa się pod BLIK*, Niebezpiecznik.pl, https://niebezpiecznik.pl/post/uwaga-ktos-podszywa-sie-pod-blik/ (dostęp 25.12.2023).

Kotliński G. (2022), *Dylematy banków spółdzielczych w dobie rewolucji cyfrowej 4.0 ze szczególnym uwzględnieniem wyzwań w sferze marketingu*, [w:] G. Kotliński (red.), *Bankowość komercyjna i spółdzielcza w Polsce – refleksje po trzech dekadach transformacji. Szkice ku pamięci Doktora Ryszarda Mikołajczaka* (s. 215–238). Poznań: Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu. https://doi.org/10.18559/978-83-8211-152-1/12

KPMG (2024), *Barometr cyberbezpieczeństwa. Na fali, czy w labiryncie regulacji?*, https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpiecze%C5%84stwa-2024.pdf (dostęp 6.04.2024).

Krzysztoszek M. (2017), *Bankowość elektroniczna w teorii i praktyce*, Komisja Nadzoru Finansowego.

Laszczak M. (2019), *Zarządzanie bezpieczeństwem w erze cyfrowej*, „Bezpieczeństwo. Teoria i Praktyka", 37(4).

Matacz M., Vodičková W. (2023), *Zjawisko phishingu w Polsce. De Securitate et Defensione*, „O Bezpieczeństwie i Obronności", 9(1).

mbank.pl (2023), *Potwierdzaj tożsamość w aplikacji mobilnej*, https://www.mbank.pl/indywidualny/aplikacja-i-serwis/pierwsze-kroki/potwierdzenie-tozsamosci/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2013), *Klienci iPKO – uwaga na phishing!*, https://niebezpiecznik.pl/post/klienci-ipko-uwaga-na-phishing/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2014), *Uwaga klienci PKO i Citi banku! Trwa potężna kampania phishingowa, z kont skradziono już kilkanaście tysięcy złotych*, https://niebezpiecznik.pl/post/uwaga-klienci-pko-i-citi-banku-trwa-potezna-kampania-phishingowa-z-kont-skradziono-juz-kilkanascie-tysiecy-zlotych/ (dostęp 6.04.2024).

Niebezpiecznik.pl (2018), *Dlaczego (nie) warto używać aplikacji mobilnej do autoryzacji przelewów?*, https://niebezpiecznik.pl/post/autoryzacja-mobilna-aplikacja-bank-przelewy/ (dostęp 15.04.2024).

Niebezpiecznik.pl (2021), *Klucze U2F – pytania i odpowiedzi. Dlaczego hakerzy ich nienawidzą i dlaczego warto z nich korzystać?*, https://niebezpiecznik.pl/post/klucze-u2f-pytania-i-odpowiedzi/ (dostęp 8.04.2024).

Niebezpiecznik.pl (2022a), *Uwaga klienci ING!*, https://niebezpiecznik.pl/post/uwaga-klienci-ing/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2022b), *Uwaga klienci mBanku!*, https://niebezpiecznik.pl/post/uwaga-klienci-mbanku-2/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2023a), *Uwaga klienci PKO!*, https://niebezpiecznik.pl/post/uwaga-klienci-pko/ (dostęp 25.12.2023).

Niebezpiecznik.pl (2023b), *Uwaga klienci banku PKO!*, https://niebezpiecznik.pl/post/uwaga-klienci-banku-ipko/ (dostęp 25.12.2023).

Oleksiewicz I. (2019), *Bezpieczeństwo informacyjne w cyberprzestrzeni a stany nadzwyczajne Rzeczypospolitej Polskiej*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie", (33), 144–153.

Piłat K., Pawłowski M.T., Kozieł G. (2022), *Analiza wiedzy o aspektach cyberbezpieczeństwa i logowania dwuetapowego w społeczeństwie*, „Journal of Computer Sciences Institute", 23.

Piotrowski Z., Różanowski K., Gajewski P. (2012), *Bezpieczeństwo połączeń w telefonii PSTN*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", 6(8).

Pisarewicz P., Podlewski J. (2023), *Cyberbezpieczeństwo polskiego sektora ubezpieczeniowego w kontekście krajowych i unijnych regulacji prawnych*, „Bank i Kredyt", 54(5).

Pitera R. (2017), *Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej*, „Przegląd Nauk o Obronności", 2(4).

pkobp.pl (2022), *Weryfikacja pracownika banku w IKO*, https://www.pkobp.pl/klient-indywidualny/aplikacja-iko-ipko/bezpieczenstwo/jak-sprawdzic-czy-dzwoni-pracownik-banku (dostęp 25.12.2023).

Popik A., Gryglicka A. (2022), *Ocena poziomu bezpieczeństwa użytkowników rachunków bankowych i analiza zachowań banków w sytuacji wystąpienia incydentu zagrożenia bezpieczeństwa*, „Finanse i Prawo Finansowe".

Rabka M. (2020), *Internet XXI wieku–pułapka zagrożeń dla dzieci, młodzieży i osób starszych w dobie pandemii Covid-19*, „Współczesne Problemy Zarządzania", 8(1(16)).

Rojek, M. (2019), *Cyberprzestrzeń jako miejsce międzypokoleniowego uczenia się. Przykład projektu „ICT Guides"*, „Problemy Opiekuńczo-Wychowawcze", 579(4).

Samcik M. (2019), *Banki w pośpiechu likwidują karty-zdrapki i... tokeny. Co się stało. że token przestał spełniać wymogi bezpieczeństwa?*, https://subiektywnieofinansach.pl/psd2-likwidacja-karty-zdrapki-token-sms-autoryzacyjny/ (dostęp 15.04.2024).

Schuetz S., Lowry P.B., Thatcher J. (2016), *Defending against spear-phishing: Motivating users through fear appeal manipulations*. In 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, June.

Sharevski F., Devine A., Pieroni E., & Jachim P. (2022), *Gone Quishing: A Field Study of Phishing with Malicious QR Code*s. arXiv preprint arXiv:2204.04086.

Singh J. (2011), *Detection of Phishing e-mail*, IJCST, 2(1).

SMSAPI (2024), *Bezpieczeństwo cyfrowe Polaków. Oszustwa internetowe i zagrożenia komunikacji mobilnej*, https://www.smsapi.pl/static/files/Bezpieczenstwo_cyfrowe_Polakow-Raport_SMSAPI_2024.pdf (dostęp 6.04.2024).

Srinivas S., Balfanz D., Tiffany E., Czeskis A. (2015), *Universal 2nd factor (U2F) overview*, „FIDO Alliance Proposed Standard", 15.

Stefanicki R. (2023), *„Mamo, miałam wypadek!". Uważaj, bo sztuczna inteligencja klonuje głos i wyłudza pieniądze*, wyborcza.biz, https://wyborcza.biz/biznes/7,177150,30152534,mamo-mialam-wypadek-uwazaj-bo-sztuczna-inteligencja-klonuje.html (dostęp 6.04.2024).

Thakur T., Verma R. (2014), *Catching classical and hijack-based phishing attacks*. In International Conference on Information Systems Security (pp. 318–337). Cham: Springer International Publishing.

Xopero. (2021), Cyberbezpieczeństwo Trendy 2021.

Xu T., Singh K., Rajivan P. (2023), *Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks*, „Applied Ergonomics", 108, 103908.

Yeboah-Boateng E.O., Amanor P.M. (2014), *Phishing, SMiShing & Vishing: an assessment of threats against mobile devices*, „Journal of Emerging Trends in Computing and Information Sciences", 5(4).

Zagańczyk M. (2019), *Bank Millennium wprowadza token sprzętowy z czytnikiem i technologią Cronto firmy OneSpan*, https://www.telepolis.pl/fintech/fintech/bank-millennium-wprowadza-token-sprzetowy-z-czytnikiem-i-technologia-cronto-firmy-onespan (dostęp 15.04.2024).

ZBP (2022), Raport: *Cyberbezpieczny portfel*, https://www.zbp.pl/getmedia/bebff99e-f5b7-4644-aec3-4ad3ff5c970a/Cyberbezpieczny_portfel_2022a (dostęp 7.04.2024).

DOI: 10.26354/bb.3.1.94.2024

Krystyna Patora*
ORCID: 0000-0003-2526-6801
krystyna.patora@wpia.uni.lodz.pl

Relacje norm prawa Unii Europejskiej i prawa krajowego w zakresie ścigania przestępstw prania brudnych pieniędzy

Streszczenie

Tematem niniejszego artykułu jest niespójność przepisów dotyczących prania „brudnych" pieniędzy w prawie krajowym, a także w relacji do prawa unijnego. W artykule zostały wskazane braki legislacyjne, które uniemożliwiają skuteczne ograniczanie przestępczości prania pieniędzy. Bez ich wprowadzenia nie będzie możliwe ograniczanie zjawiska prania brudnych pieniędzy, szczególnie w tych wypadkach, a jest ich coraz więcej, przestępczości transgranicznej oraz popełnianej z wykorzystaniem podmiotów zbiorowych.

Słowa kluczowe: pranie brudnych pieniędzy, czyn zabroniony, korzyści związane z popełnieniem czynu zabronionego, przestępczość zorganizowana, okoliczności obciążające, zabezpieczenie majątkowe, dyrektywy

Kody JEL: K14

Relations between the norms of European Union law and national law in the area of the Prosecuting of Money Laundering Offences

Abstract

The subject of this article is the inconsistency of provisions regarding money laundering between the domestic law and the EU law. The article discusses the legislative shortcomings that prevent the effective control of money laundering crimes. Without its introduction, it will not be possible to limit the phenomenon of money laundering especially in these cases. And there are more and more of them, cross border crimes and crimes commited using collective entities.

Keywords: money laundering, prohibited act, proceeds of crime, organised crime, aggravating circumstances, asset-based security, directives

JEL Codes: K14

* Krystyna Patora – Uniwersytet Łódzki, Wydział Prawa i Administracji.

Wstęp

Przestępczość związana z tzw. praniem pieniędzy, czyli pożytkowaniem korzyści, które zostały uzyskane z czynów zabronionych, stanowi przedmiot zainteresowania ustawodawstw krajowych, a także międzynarodowych. Celem wprowadzenia znamion czynów prania „brudnych" pieniędzy było pozbawienie sprawców przestępstw korzyści, jakie uzyskiwali początkowo z przestępczości zorganizowanej, a następnie każdego rodzaju tej przestępczości. Taki proces można zaobserwować w prawie krajowym poszczególnych państw. Przy globalizacji obrotu, sposobności wykorzystania Internetu w przestępczości i możliwości popełnienia przestępstw związanych z praniem brudnych pieniędzy, osiąganie ograniczenia tego zjawiska możliwe jest tylko dzięki współpracy pomiędzy poszczególnymi krajami. Zacieśnienie tej współpracy musi następować w pierwszej kolejności w obszarze systemu bankowego, ponieważ to on jest najczęściej używany do dokonywania transferów środków pochodzących z przestępczości. Konieczne jest więc omówienie najnowszych rozwiązań w tym zakresie, aby pokazać, czy są one spójne, a jeśli nie, to czy powinny być dokonane kolejne zmiany, które będą skutkować ich zgodnością.

1. Przestępstwo „prania brudnych pieniędzy" w prawie międzynarodowym oraz unijnym

Pojęcie „prania brudnych pieniędzy" po raz pierwszy zostało użyte w latach 20. XX wieku i dotyczyło mafii chicagowskiej (Wąsowski 2001, s. 9). Chodziło o nielegalną, zabronioną przez prawo (Wójcik 2002, s. 23), działalność związaną z produkcją alkoholu, która przynosiła ogromne dochody. Aby ta nielegalna działalność w postaci produkcji alkoholu była trudna do wykrycia, organizacje zajmujące się nią prowadziły jednocześnie legalnie działające pralnie, sklepy spożywcze czy cukiernie, których dochody były w rzeczywistości bardzo skromne i mieszały ogromne dochody z nielegalnej działalności z dochodami z działalności legalnej (Pływaczewski 1993, s. 33). Miało to na celu utrudnienie lub uniemożliwienie ustalenia ich pochodzenia. Pranie pieniędzy wywodzi się więc z zakazanej działalności, przynoszącej ogromne zyski, które były wykazywane w legalnie działających podmiotach, w tym szczególnie w osławionych pralniach. W takim otoczeniu została stworzona definicja „prania brudnych pieniędzy", która została opracowana przez Ośrodek Szkolenia Departamentu Skarbu USA i zgodnie z którą „praniem brudnych pieniędzy" jest: „proces, przy pomocy którego dochody przypuszczalnie uzyskane z działalności przestępczej są przekazywane, przekształcane, wymieniane albo też łączone i mieszane z legalnymi funduszami w celu ukrycia lub zatajenia prawdziwego charakteru, źródła, ukierunkowania, przepływu lub własności tych dochodów. Celem procesu prania pieniędzy jest nadanie pozorów legalności *środkom* uzyskanym z działalności pozaprawnej lub działań z nią związanych" (Wójcik 2002, s. 23–24). Pierwsze regulacje pojawiły się w Stanach Zjednoczonych w latach 70. XX wieku (Bank Secrecy Act of 1970 r., 84 Stat. 1114), a ustawa o zwalczaniu prania pieniędzy

zaczęła obowiązywać w 1986 r. (Gilmore 1999, s. 27). Natomiast zwrot „pranie pieniędzy" został użyty w 1982 r. w sprawie *United States of America v 4 255 625,39 USD* (Gilmore 1999, s. 26). Istotą przestępczości w postaci prania brudnych pieniędzy jest więc ukrywanie istnienia nielegalnie pozyskanych dochodów i ich nielegalne użytkowanie, poprzez nadanie tym procesom pozorów legalności (Definicja z *The Cash Connection, Organized Crime and Money Laudering*, 1984 r., nr 7, powołana przez Górniok 2003, s. 96; także Górniok 2000, s. 47).

R. Lizak pisze, że cechą wspólną wszystkich definicji jest to, że „pranie brudnych pieniędzy" polega na legalizowaniu dochodów pochodzących z działalności niezgodnej z prawem (Lizak 2018, s. XII).

Problem „prania brudnych pieniędzy" został na arenie międzynarodowej oraz europejskiej zauważony dość szybko. Jedną z pierwszych inicjatyw były Zalecenia Komitetu Ministrów Rady Europy z 27.06.1980 r. w sprawie przeciwdziałania transferowi i ukrywaniu funduszy pochodzących z przestępstw „prania brudnych pieniędzy" (Committee of Ministers of the Council of Europe, *Recommendation No. R (80) 10 on measures against the transfer and the safekeeping of funds of criminal origin*, 27.06.1980). 20.12.1988 r. została sporządzona w Wiedniu Konwencja Narodów Zjednoczonych o zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi (Konwencja Narodów Zjednoczonych o zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi, sporządzona w Wiedniu 20.12.1988 r., Dz.U. 1995 Nr 15, poz. 69 z 20.02.1995), zwana także Konwencją wiedeńską, która zawierała definicję „prania brudnych pieniędzy".

Niedługo potem została przyjęta Konwencja Nr 141 Rady Europy z 8.11.1990 r. o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa (Konwencja Nr 141 o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa, ratyfikowana przez Polskę w 2000 r. (Dz.U. 2003 Nr 46, poz. 394).

Z punktu widzenia ważności aktów prawnych dla ograniczania przestępczości prania „brudnych" pieniędzy należy wymienić, wprawdzie już nie obowiązującą, ale mającą ważne znaczenie, Dyrektywę Rady 91/308/EWG z 10.06.1991 r. w sprawie uniemożliwienia korzystania z systemu finansowego w celu prania pieniędzy, która w art. 1 stanowiła, że praniem „brudnych" pieniędzy było wymienione poniżej umyślne postępowanie, dokonywane w celu:

- konwersji lub przekazania mienia, ze świadomością, że pochodzi ono z działalności przestępczej lub z udziału w takiej działalności, celem ukrywania lub zatajania bezprawnego pochodzenia tego mienia, albo udzielania pomocy osobie, która bierze udział w takiej działalności, aby uniknęła ona prawnych konsekwencji tych działań,
- ukrycia lub zatajenia prawdziwego charakteru, źródła, miejsca przechowywania, przemieszczaniu, praw związanych z tym mieniem lub jego własnością, ze świadomością, że źródłem tego mienia jest działalność o charakterze przestępczym lub udział w takiej działalności,

- nabycia, posiadania albo używania mienia, ze świadomością w momencie jego otrzymania, że mienie to pochodzi z działalności o charakterze przestępczym lub udział w takiej działalności,
- udziału, współdziałania w celu popełnienia, usiłowanie popełnienia, jak też pomocnictwo, nakłanianie, ułatwianie oraz doradzanie w przypadku czynów określonych w powyższych podpunktach (Dyrektywa Rady 91/308/EWG z 10.06.1991 r. w sprawie uniemożliwienia korzystania z systemu finansowego w celu prania pieniędzy – Dz.U.UE L z 28.06.1991 r., Dz.U.UE.L.1991.166.77).

Wskazanie rozumienia określenia *działalności przestępczej* nastąpiło w art. 3 ust. 1 lit a Konwencji wiedeńskiej[1] i obejmowało wszystkie inne typy działalności przestępczej określone do celów dyrektywy przez każde Państwo Członkowskie (Dyrektywa Rady 91/308/EWG z 10.06.1991 r. w sprawie uniemożliwienia korzystania z systemu finansowego w celu prania pieniędzy – Dz.U.UE L z 28.06.1991 r., Dz.U.UE.L.1991.166.77).

Istotne znaczenie ma także Konwencja Narodów Zjednoczonych z 15.11.2000 r. przeciwko międzynarodowej przestępczości zorganizowanej (Konwencja Narodów Zjednoczonych z 15.11.2000 r. przeciwko międzynarodowej przestępczości zorganizowanej – Dz.U. 2005 Nr 18, poz. 158 z 31.01.2005), ponieważ rozszerzyła ona w art. 6 penalizację prania dochodów z przestępstwa, w porównaniu do Konwencji wiedeńskiej.

Na podstawie art. 1.3. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z 20.05.2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającej rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającej dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE Dz.U.UE L z 5.06.2015 r., za pranie pieniędzy uznane są następujące czyny popełnione umyślnie:

a) konwersja lub przekazywanie mienia, ze świadomością, że pochodzi ono z działalności przestępczej lub z udziału w takiej działalności, w celu ukrywania lub zatajania nielegalnego pochodzenia tego mienia lub udzielenia pomocy dowolnej osobie, która bierze udział w takiej działalności, dla umożliwienia tej osobie uniknięcia konsekwencji prawnych takiego działania;
b) ukrycie lub zatajenie prawdziwego charakteru mienia, jego źródła, miejsca położenia, rozporządzania nim, przemieszczania, praw odnoszących się do mienia lub własności mienia, ze świadomością, że mienie to pochodzi z działalności przestępczej lub z udziału w takiej działalności;

[1] W art. 3 ust. 1 lit. a Konwencji Narodów Zjednoczonych o zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi, sporządzonej w Wiedniu 20.12.1988 r. – Dz.U. z 20.02.1995 r., Dz.U.1995.15.69 zał., jako wchodzące w skład działalności przestępczej zostały wskazane dokonane umyślnie wyrób, wytwarzanie, sporządzanie wyciągów lub preparatów, oferowanie, proponowanie sprzedaży, rozprowadzanie, sprzedawanie, dostarczanie na wszelkiego rodzaju warunkach, pośredniczenie, wysyłanie, przesyłanie w tranzycie, przewożenie, wywóz, bądź przywóz każdego środka odurzającego, bądź każdej substancji psychotropowej, dokonywane niezgodnie z postanowieniami Konwencji z 1961 r., Konwencji z 1961 r. z późniejszymi zmianami, bądź Konwencji z 1971 r.

c) nabycie, posiadanie lub użytkowanie mienia, ze świadomością w momencie jego otrzymania, że mienie to pochodzi z działalności przestępczej lub z udziału w takiej działalności;
d) udział lub współdziałanie w popełnieniu, usiłowanie popełnienia oraz pomocnictwo, podżeganie, ułatwianie oraz doradzanie przy popełnieniu któregokolwiek z czynów, o których mowa w lit. a), b) i c) (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z 20.05.2015 r. w sprawie zapobiegania wykorzystywaniu 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.U.UE L z 5.06.2015 r., Dz.U.UE.L.2015.141.73 ze zm.).

Dyrektywa ta zawiera w art. 3 pkt 4 w zw. z art. 3 pkt 4 lit. f, definicję *działalności przestępczej*, przez którą rozumiano jakikolwiek przestępczy udział w popełnieniu poważnych przestępstw, w tym między innymi przestępstw podatkowych odnoszących się do podatków bezpośrednich i pośrednich – zgodnie z definicją w prawie krajowym państw członkowskich – których maksymalne zagrożenie karą przekraczało rok pozbawienia wolności lub ograniczenia wolności, lub – w przypadku państw członkowskich, których systemy prawne określają w odniesieniu do przestępstw minimalny próg zagrożenia karą – wszystkich przestępstw, których dolna granica zagrożenia karą jest wyższa niż sześć miesięcy pozbawienia wolności lub ograniczenia wolności (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z 20.05.2015 r. w sprawie zapobiegania wykorzystywaniu 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.U.UE L z 5.06.2015 r., Dz.U.UE.L.2015.141.73 ze zm.).

2. Przestępstwo prania brudnych pieniędzy w polskim prawie w ujęciu historycznym

W Polsce, podobnie jak na świecie, to system bankowy najczęściej wykorzystywany był do prania pieniędzy pochodzących z tzw. przestępstw bazowych.

Dlatego to banki jako pierwsze dostrzegały nowe formy tej przestępczości i opracowywały zalecenia dotyczące ograniczania wykorzystywania ich systemów do ukrywania korzyści pochodzących z popełniania przestępstw gospodarczych, ale i kryminalnych. Początkowo ograniczanie odbywało się za pomocą różnego rodzaju obostrzeń o charakterze administracyjnym. Określenie „prania brudnych pieniędzy" po raz pierwszy zostało użyte w Zarządzeniu nr 16/92 Prezesa NBP z 1.10.1992 r. w sprawie zasad postępowania banków w razie ujawnienia okoliczności wskazujących na lokowanie w banku środków pieniężnych lub innych wartości majątkowych pochodzących lub mających związek z przestępstwem oraz przy

dokonywaniu wpłat gotówkowych przekraczających określoną kwotę, gdzie w paragrafie 1 wskazano, że przez „pranie brudnych pieniędzy" należy rozumieć: „sytuację, która zachodzi wówczas, gdy ujawnione okoliczności wskazują, że lokowane w banku środki pieniężne lub inne wartości majątkowe pochodzą z przestępstwa lub uczestnictwa w jego popełnieniu, albo że ich pochodzenie, stan lub przeznaczenie mają zostać ukryte z przyczyn mających związek z przestępstwem" (Zarządzenie nr 16/92 Prezesa Narodowego Banku Polskiego z 1.10.1992 r. w sprawie zasad postępowania banków w razie ujawnienia okoliczności wskazujących na lokowanie w banku środków pieniężnych lub innych wartości majątkowych pochodzących lub mających związek z przestępstwem oraz przy dokonywaniu wpłat gotówkowych przekraczających określoną kwotę Dz.Urz. NBP z 2.10.1992 r., 20.09.1992). Była to jednak tylko jedna, przysłowiowa, strona medalu, ponieważ należało, dla skutecznej walki z tym zjawiskiem, wprowadzić przepisy uznające tego typu zachowania jako czyny zabronione zagrożone sankcjami karnymi, co też zostało po raz pierwszy uczynione w art. 5 ustawy z 12.10.1994 r. o ochronie obrotu gospodarczego i zmianie niektórych przepisów prawa karnego (Ustawa z 12.10.1994 r. o ochronie obrotu gospodarczego i zmianie niektórych przepisów prawa karnego – Dz.U. Nr 126, poz. 615). Ograniczyło się ono do środków płatniczych, papierów wartościowych lub wartości dewizowych, pochodzących ze zorganizowanej przestępczości powiązanej z obrotem środkami odurzającymi lub psychotropowymi, fałszowaniem pieniędzy lub papierów wartościowych, wymuszeniem okupu albo handlu bronią, co do których zakazano: przyjmowania, przenoszenia własności, posiadania, przekazywania, wywożenia za granicę albo podejmowania innych działań, które mogły udaremnić stwierdzenie ich przestępczego pochodzenia, wykrycie albo orzeczenie przepadku. Zachowania miały być podejmowane w celu wprowadzenia opisanych przedmiotów czynności wykonawczych do legalnego obrotu. Pierwotnie przestępstwo prania „brudnych" pieniędzy zostało powiązane ze zorganizowaną przestępczością (Buchała i in. 1995, s. 82), co znacznie ograniczyło możliwości jego zwalczania, szczególnie co do korzyści pochodzących z przestępczości gospodarczej, która na początku lat 90. była szczególnie rozległa w Polsce. Jej gwałtownemu rozwojowi sprzyjały przeobrażenia gospodarcze i brak odpowiednich regulacji dotyczących typowych dla rodzącej się gospodarki rynkowej przestępstw.

Trzeba podkreślić, że polski ustawodawca długo nie zdecydował się na wprowadzenie do prawa karnego legalnej definicji przestępstwa prania pieniędzy. Obecnie obowiązująca ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – Dz.U. 2023, poz. 1124), w artykule 2.2. pkt 14, wskazuje, że przez pranie brudnych pieniędzy rozumie się czyn określony w art. 299 ustawy z 6.06.1997 r. – Kodeks karny. Zgodnie z art. 299 § 1 Kodeksu karnego karalne jest podejmowanie wymienionych w tym przepisie czynności sprawczych do środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych lub innego mienia ruchomego lub nieruchomości, pochodzących z korzyści związanych z popełnieniem czynu zabronionego (Ustawa z 6.06.1997 r. Kodeks karny – t.j. Dz.U. 2022, poz. 1138).

W kodeksie karnym z 1997 r. przestępstwo prania brudnych pieniędzy uregulowane zostało w art. 299 § 1 kodeksu karnego. Przepis ten był wielokrotnie nowelizowany, przy czym zmiany generalnie polegały na dodawaniu nowych czynności sprawczych, stanowiących kolejne formy prania pieniędzy. Wszelkie wprowadzane zmiany miały przede wszystkim na celu to, aby objęto penalizacją kolejne występujące w rzeczywistości zachowania, które zmierzały do wykorzystania owoców przestępstw. Praktyka ujawniała nowe niekorzystne zjawiska, które były szkodliwe, ale prawnie irrelewantne, a ustawodawca tak zmieniał przepisy dotyczące prania brudnych pieniędzy, aby kolejne zachowania uznać za przestępstwa i objąć odpowiedzialnością karną. Dlatego należy wspomnieć tylko o najważniejszych zmianach art. 299 kodeksu karnego.

Pierwszym poważnym krokiem mającym na celu poszerzenie pola kryminalizacji było zastąpienie w treści art. 299 § 1 kodeksu karnego określenia: *pochodzące z korzyści związanych z popełnieniem przestępstwa przez inne osoby* określeniem: *pochodzące z korzyści związanych z popełnieniem czynu zabronionego*, co miało miejsce na podstawie nowelizacji omawianego przepisu w 2000 r. (Ustawa z 16.11.2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – Dz.U. 2017, poz. 1049). W ten sposób zlikwidowany został wymóg, aby czyn pierwotny był popełniony przez inną osobę niż ta która dopuszczała się prania korzyści pochodzących z czynu bazowego. Ta zmiana legislacyjna poszerzyła zakres podmiotowy sprawców czynów z art. 299 § 1 k.k. o tych, którzy dopuścili się przestępstw bazowych, z których korzyści pochodziły.

Wówczas weszła w życie ustawa z 16.11.2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Ustawa z 16.11.2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – Dz.U. 2017, poz. 1049), która regulowała zasady oraz tryb przeciwdziałania praniu pieniędzy, przeciwdziałania finansowaniu terroryzmu, stosowania szczególnych środków ograniczających przeciwko osobom, grupom i podmiotom oraz obowiązki podmiotów uczestniczących w obrocie finansowym w zakresie gromadzenia i przekazywania informacji. W art. 2 pkt 9 ustawy umieszczona została definicja „prania pieniędzy", która obejmowała czynności polegające na:

a) zamianie lub przekazaniu wartości majątkowych pochodzących z działalności o charakterze przestępczym lub z udziału w takiej działalności, w celu ukrycia lub zatajenia bezprawnego pochodzenia tych wartości majątkowych albo udzieleniu pomocy osobie, która bierze udział w takiej działalności w celu uniknięcia przez nią prawnych konsekwencji tych działań,
b) ukryciu lub zatajeniu prawdziwego charakteru wartości majątkowych lub praw związanych z nimi, ich źródła, miejsca przechowywania, rozporządzania, faktu ich przemieszczania, ze świadomością, że wartości te pochodzą z działalności o charakterze przestępczym lub udziału w takiej działalności,
c) nabyciu, objęciu w posiadanie albo używaniu wartości majątkowych pochodzących z działalności o charakterze przestępczym lub udziału w takiej działalności,
d) współdziałaniu, usiłowaniu popełnienia, pomocnictwie lub podżeganiu w przypadkach zachowań określonych w lit. a–c.

Ustawa weszła w życie 23.06.2001 r., a została uchylona 13.07.2018 r., kiedy to weszła w życie kolejna ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (Ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu – t.j. Dz.U. 2023, poz. 1124), która obowiązuje do dziś.

Nowelizacją z 25.06.2009 r., która weszła w życie 22.10.2009 r. (Ustawa z 25.06.2009 r. o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw – Dz.U. 2009 Nr 166, poz. 1317) dodano w art. 299 § 1 kodeksu karnego określenia *instrumenty finansowe*, *lub inne* do mienia, a także *nieruchomości*. Była to istotna zmiana, która znacznie rozszerzyła pole kryminalizacji.

Natomiast nowelizacją z 9.10.2015 r. (Ustawa z 9.10.2015 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw – Dz.U. 2015, poz. 1855), która weszła w życie 13.02.2016 r. katalog czynności sprawczych poszerzono o posiadanie, używanie, ukrywanie, konwersję lub transfer korzyści. Nowela ta ponadto wprowadzała nowy art. 299 § 6a k.k., tj. karalność przygotowania do popełnienia przestępstw z art. 299 § 1 i 2 k.k.

Ostatecznie czyn z art. 299 § 1 kodeksu karnego został tak skonstruowany, że przedmiot wykonawczy prania, tj.: środki płatnicze, instrumenty finansowe, papiery wartościowe oraz inne wskazane w treści tego przepisu, nie muszą pochodzić ze zorganizowanej przestępczości i mogą obejmować każdy rodzaj przestępczości, zarówno kryminalnej, jak i gospodarczej. Oznacza to, że konieczne jest rozważanie wykorzystania korzyści uzyskanych z każdego rodzaju przestępczości, co skutkuje badaniem związanym z ustalaniem stanu majątkowego podejrzanych o popełnienie praktycznie każdego rodzaju przestępczości.

Obecna regulacja, umieszczona w art. 299 § 1 kodeksu karnego, pomimo wielokrotnych nowelizacji nie jest jednak doskonała. Problemem, który systematycznie w teorii oraz w praktyce ma istotne znaczenie jest to, że przedmiot wykonawczy musi pochodzić z korzyści związanych z popełnieniem czynu zabronionego. Trzeba podkreślić, że w pierwszej kolejności chodzi o każdy czyn zabroniony. Pojęcie „czynu zabronionego" zostało zdefiniowane jako „zachowanie o znamionach określonych w ustawie karnej" (Ustawa z 6.06.1997 r. Kodeks karny – t.j. Dz.U. 2017 poz. 2204 ze zm.). Definicja pojęcia „czynu zabronionego" została także wskazana w art. 53 § 1 Kodeksu karnego skarbowego (Ustawa z 10.09.1999 r. Kodeks karny skarbowy – t.j. Dz.U. 2021, poz. 408). W doktrynie reprezentowany jest pogląd, że pojęcie „czynu zabronionego" z art. 299 § 1 k.k. nie obejmuje czynów zabronionych wskazanych w kodeksie karnym skarbowym (Zoll 2016, s. 691–692; podobnie Wróbel 2012, s. 104 i nast.; Michalska-Warias 2016, s. 133–139). W doktrynie pojawiły się także poglądy przeciwne, zgodnie z którymi pranie pieniędzy obejmuje czyny zabronione, które zostały wskazane w kodeksie karnym skarbowym (Błachnio 2024, teza 15; Oczkowski 2023, teza 7; Giezek 2021, teza 35; Gałązka 2024, s. 1799; Potulski 2023/Legalis/teza nr 2, notka na marginesie nr 13; Gadecki 2023, s. 896; Zawłocki, Gałęski 2024/Legalis, teza nr 14, IV. Strona przedmiotowa typu czynu

zabronionego z § 1, notka na marginesie nr 50). Stanowisko takie wyraził także SN w uchwale z 4.04.2005 r., sygn. I KZP 7/05, OSNKW 2005/5/44, a także w postanowieniu z dnia 12.01.2015 r., sygn. III KK 247/14, Lex nr 1622321. Postanowienie to zostało zaakceptowane przez M. Czepukojcia (Czepukojć 2017, s. 64–71). Również w kolejnym postanowieniu z 30.11.2017 roku, IV KK 272/17, SN przyjął, że przestępstwem bazowym jest każde przestępstwo, z którego pochodzą dochody. Tak więc wydaje się, że w doktrynie i orzecznictwie sądowym przeważa stanowisko, iż czynem bazowym może być czyn określony w kodeksie karnym skarbowym.

Oznacza to, że konieczne jest uprawdopodobnienie popełnienia uprzednio czynu zabronionego tak zwanego „bazowego" co najmniej w zakresie ustalenia stanu faktycznego oraz odpowiedniej kwalifikacji prawnej. Jest to warunek konieczny do tego, aby możliwe było w dalszej kolejności przypisanie przestępstwa prania brudnych pieniędzy. Oznacza to, że korzyści z popełnienia czynu zabronionego nie mogą pochodzić z – przykładowo – nieujawnionych źródeł, a więc wtedy, gdy ujawnione zostały nadmierne dochody, ale nie jest możliwe ustalenie, że stanowiące je środki pochodzą z czynu zabronionego. Już na etapie tych rozważań można wskazać, że pojęcie „czynu zabronionego", użyte w art. 299 § 1 kodeksu karnego, nie jest tożsame z pojęciem „przestępstwa", użytego do wyjaśnienia definicji „działalności przestępczej" z art. 3 pkt 4 w zw. z art. 3 pkt 4 lit. f Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z 20.05.2015 r. sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającej rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającej dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE Dz.U.UE L z 5.06.2015 r. Wydaje się, że, z jednej strony definicja z art. 3 pkt 4 w zw. z art. 3 pkt 4 lit. f Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z 20.05.2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu była początkowo szersza niż w prawie polskim, ponieważ obejmowała również korzyści pochodzące z przestępstw podatkowych, ale obecnie zakres ten jest podobny, a, z drugiej strony, w prawie polskim brak jest ograniczenia w zakresie zagrożenia ustawowego, co będzie skutkowało szerszym wyznaczeniem granic przestępstw bazowych w prawie polskim.

Ponadto w polskim orzecznictwie sądowym powstał spór co do wykładni znamienia *pochodzące z korzyści związanych z popełnieniem czynu zabronionego*.

W orzecznictwie sądowym wskazywano, że: *pochodzące z korzyści związanych z popełnieniem czynu zabronionego* oznacza wartości majątkowe uzyskane za pomocą czynu zabronionego i obejmujące te wartości majątkowe, których nie posiadałby sprawca pierwotny, gdyby nie dopuścił się tego czynu (Postanowienie SA w Katowicach z 15.07.2009 r., II AKz 417/09, KZS 2010/11/55, OSA 2010/7/3-10). Przyjmowano szerokie rozumienie korzyści pochodzących z przestępstwa jako wartości majątkowych pochodzących z popełnienia czynu zabronionego, a także wartości, której podstawę stanowi stosunek prawny powstały w wyniku zabronionych prawnie zabiegów (Wyrok SA w Krakowie z 28.10.2009 r., II AKa 184/09, KZS 2009/12/61).

Odnośnie do bezpośredniego lub pośredniego pochodzenia z korzyści związanych z popełnieniem czynu zabronionego zarysowały się w orzecznictwie sądowym trzy stanowiska. Na podstawie pierwszego z nich, wyrażonego w wyroku Sądu Apelacyjnego w Katowicach z 15.07.2009 r., nie jest istotne, czy dane wartości majątkowe pochodzą bezpośrednio, czy tylko pośrednio z owego pierwotnego czynu zabronionego (Wyrok SA w Katowicach z 15.07.2009 r, II AKa 417/09, KZS 2009/9/70). Innego zdania był Sąd Najwyższy, który w wyroku z 1.09.2010 r., V KK 43/10, wskazał, że chodzi tylko o korzyści, które pochodzą tylko pośrednio z popełnienia czynu zabronionego. Nie dotyczy to tych korzyści, które zostały uzyskane za pomocą czynu zabronionego. Podobnego zdania był Sąd Apelacyjny w Łodzi (Wyrok SA w Łodzi z 13.12.2012 r., II AKa 198/12; KZS 2014/11/53/). Mogłoby się wydawać, że do pewnego ujednolicenia orzecznictwa sądowego doszło w związku z wydaniem uchwały Sądu Najwyższego w 2013 r. W uchwale 7 Sędziów z 18.12.2013 r. Sąd Najwyższy wskazał, że chodzi zarówno o korzyści pochodzące bezpośrednio, jak i pośrednio z popełnienia czynu zabronionego (Uchwała 7 Sędziów SN (zasada prawna) z 18.12.2013 r., I KZP 19/13, OSNKW 2014, Nr 1, poz. 1).

Jeżeli chodzi o doktrynę to skłaniała się do przyjmowania pochodzenia bezpośredniego oraz pośredniego korzyści. Jacek Giezek stwierdził, że za nieracjonalne należałoby uznać oczekiwanie, by uzyskane z czynu zabronionego pieniądze miały najpierw podlegać bezkarnemu przetworzeniu, by dopiero wówczas stać się przedmiotem karalnego ich legalizowania. Skoro przestępstwem jest podejmowanie opisanych w dyspozycji art. 299 § 1 kodeksu karnego czynności w stosunku do praw i rzeczy pochodzących z korzyści związanych z popełnieniem czynu pośrednio, to tym bardziej zabronione jest podejmowanie takich czynności w stosunku do środków majątkowych pochodzących z czynu zabronionego bezpośrednio (Giezek 2013). Jerzy Duży uważa, że przyjęcie tezy o konieczności wykazania pośredniego związku korzyści z zabronionym czynem pierwotnym dla wyczerpania znamion przestępstwa z art. 299 § 1 k.k. uczyniłoby w polskich realiach art. 299 § 1 k.k. przepisem martwym. Miałoby to określone konsekwencje międzynarodowe w postaci braku przestrzegania Konwencji Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzonej w Warszawie 16.05.2005 r. (Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzona w Warszawie 16.05.2005 r. – Dz.U. 2008 Nr 165, poz. 1028). Zgodnie z art. 1a Konwencji dochody oznaczały każdą korzyść ekonomiczną pochodzącą lub uzyskaną bezpośrednio lub pośrednio z przestępstw (Duży 2010). Takie samo stanowisko jest reprezentowane przez B. Piątkowską oraz K. Skelnik (Piątkowska i Skelnik 2022, s. 207). Tak więc niezależnie od powyższych sporów w polskim prawie karnym czynem bazowym prania brudnych pieniędzy może być każdy czyn zabroniony, z którego pochodzą korzyści. Takie stwierdzenie ma istotne znaczenie w zakresie międzynarodowej współpracy w zakresie odzyskiwania mienia na podstawie Dyrektywy Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotyczącej współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzą-

cych z przestępstwa lub innego mienia związanego z przestępstwem (Dyrektywa Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem – Dz.U.UE.L.2007.332.103 z dnia 18.12.2007).

Rys historyczny rozwoju regulacji prawnych na świecie i w Polsce prowadzi do wniosku, że tego typu przestępczość jest szczególnie niebezpieczna w każdym kraju i dla skutecznego jej ograniczania należy wypracowywać wspólne i spójne rozwiązania prawne tym bardziej, że będą one obowiązywać w tych państwach.

3. Dyrektywy w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych

Jeżeli chodzi o kierunek zmian prawnych w obrocie międzynarodowym, to wytyczały go dyrektywy, za którymi dopiero dokonywano nowelizacji przepisów prawa karnego, uznających kolejne zachowania za przestępstwa prania pieniędzy (ramy artykułu nie pozwalają jednak na ich omówienie). Uwagi te nie dotyczą jednak Dyrektywy Parlamentu Europejskiego i Rady w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych, która została uchwalona 23.10.2018 r. (dalej: Dyrektywa Parlamentu Europejskiego i Rady z 23.10.2018 r.) (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1673 z 23.10.2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych – Dziennik Urzędowy Unii Europejskiej z 12.11.2018 r., L 2018.284/22, weszła w życie 2.12.2018 roku). Celem tej Dyrektywy było usunięcie różnic pomiędzy poszczególnymi krajami członkowskimi w obszarze definiowania zjawiska prania pieniędzy oraz sankcji grożących za tego typu czyny zabronione (Wahl 2021).

Regulacje, które zostały zawarte w Dyrektywie, wydają się jednak iść w przeciwnym, do założonego, kierunku.

Wprawdzie w art. 1 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r. wskazano, że ustanawia ona minimalne normy dotyczące definicji przestępstw i kar w dziedzinie prania pieniędzy, jednak już definicja działalności przestępczej, zawarta w art. 2 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r., budzi wątpliwości, ponieważ w przypadku państw członkowskich, których systemy prawne określają w odniesieniu do przestępstw minimalny próg zagrożenia karą, obejmuje takie przestępstwa, w stosunku do których dolna granica zagrożenia karą jest wyższa niż sześć miesięcy pozbawienia wolności lub aresztu. Zgodnie z art. 37 kodeksu karnego kara pozbawienia wolności trwa najkrócej miesiąc. W kodeksie karnym można znaleźć wiele przepisów, gdzie dolna granica jest niższa niż 6 miesięcy, czego przykładem mogą być czyny zabronione skierowane przeciwko wierzycielom z art. 300 kodeksu karnego do artykułu 302 kodeksu karnego, z wyjątkiem art. 300 § 3 kodeksu karnego, a jednocześnie te czyny zabronione nie należą do katalogu, o którym niżej mowa.

Natomiast jeśli chodzi o karę aresztu, to jest ona przewidziana w prawie polskim w odniesieniu do wykroczeń i zgodnie z art. 18 pkt 1 kodeksu wykroczeń wynosi ona od 5 do 30 dni (Ustawa z 20.05.1971 r. Kodeks wykroczeń – Dz.U. 2021, poz. 2008). W tym miejscu należałoby odnieść się do tego, czy pojęcie „czynu zabronionego" z art. 299 § 1 k.k. odnosi się do czynu uznanego za wykroczenie. Zgodnie z art. 1 § 1 k.w. wykroczeniem jest czyn społecznie szkodliwy, zabroniony przez ustawę obowiązującą w czasie jego popełnienia pod groźbą kary aresztu, ograniczenia wolności, grzywny do 5000 zł lub nagany. Należy przywołać treść art. 3 ust. 5 Dyrektywy VI, z którego wynika, że czyny zabronione prania pieniędzy winny podlegać karze jak przestępstwa. Choć dyrektywa wyznacza warunki, na które Państwa się zgadzają, co nie oznacza, że każde Państwo nie może rozszerzyć zakresu karalności za pranie pieniędzy, to jednak prowadzi do wniosku, że może dochodzić do niespójności w zakresie obszaru penalizacji prania brudnych pieniędzy w różnych krajach i zawsze konieczne będzie porównywanie przepisów art. 299 k.k. z innymi rozwiązaniami w kierunku ustalenia, czy konkretny czyn jest czynem zabronionym w rozumieniu art. 299 § 1 k.k.

Drugim elementem definicji jest wskazanie 22 kategorii działalności przestępczej, która ma być zaliczana do przestępstw prania pieniędzy, bez względu na kryterium zagrożenia.

Grupa ta obejmuje następujące kategorie:

1) udział w zorganizowanej grupie przestępczej i wymuszenia;
2) terroryzm;
3) handel ludźmi i przemyt nielegalnych migrantów;
4) wykorzystywanie seksualne;
5) nielegalny handel narkotykami i substancjami psychotropowymi;
6) nielegalny handel bronią;
7) nielegalny handel towarami skradzionymi i innymi towarami;
8) korupcja;
9) oszustwa;
10) fałszowanie pieniądza;
11) podrabianie i piractwo produktów;
12) przestępstwa przeciwko środowisku;
13) zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu;
14) uprowadzenie, bezprawne pozbawienie wolności i wzięcie zakładnika;
15) rozbój lub kradzież;
16) przemyt;
17) przestępstwa podatkowe;
18) wymuszenie;
19) fałszowanie;
20) piractwo;
21) wykorzystywanie informacji wewnętrznych i manipulacja na rynku;
22) cyberprzestępstwa.

Z jednej strony należy zastrzec, że tworzenie wspólnego prawa jest bardzo trudnym procesem ze względu na wieloletnie kształtowanie się prawa karnego jako prawa krajowego. Z drugiej strony należy zauważyć, że prawo w obszarze karnym jest tworzone po to, aby państwa kształtowały swoje ustawodawstwo tak, by uzyskać praktyczny cel w postaci ujednolicenia w zakresie ścigania. O istotności rozwiązań dot. VI Dyrektywy może świadczyć fakt, że Zjednoczone Królestwo, pomimo wyjścia z Unii Europejskiej, opowiedziało się za wprowadzeniem regulacji wskazanych w VI Dyrektywie, o czym pisze S. Chatee (Chatee 2022). Ma to szczególny wymiar tam, gdzie chodzi o regulacje dotyczące przestępczości prania pieniędzy. Pisze o tym D. Ward (Ward 2021). Trzeba podkreślić, że w Dyrektywie Parlamentu Europejskiego i Rady z 23.10.2018 r. użyto nazewnictwa opisowego czynów zabronionych i to bardzo ogólnie wskazanych, co także będzie prowadziło do rozbieżności w zakresie uznania, jakie czyny zabronione będą zaliczane do przestępstw prania pieniędzy, bez względu na wymóg zagrożenia. Może dochodzić tutaj do niespójności, ponieważ ogólne nazewnictwo nie będzie obejmowało konkretnych czynów zabronionych, czego przykładem może być wskazane w pkt 21 „wykorzystywanie informacji wewnętrznych i manipulacja na rynku". W polskim prawie karnym brak jest tak określonego czynu zabronionego. Ponadto wątpliwości interpretacyjne będą budziły takie określenia, jak „informacja wewnętrzna" czy „manipulacja". Możliwe jest, że ten opis czynu zabronionego będzie obejmował częściowo znamiona kilku czynów zabronionych, co z punktu widzenia zasady określoności znamion czynu zabronionego, stoi na przeszkodzie uznania, że mamy do czynienia w polskim prawie z tak określonym czynem zabronionym. Trzeba wskazać, że podstawową zasadą wykładni w prawie polskim jest wykładnia językowa, która nie może być przełamana przez wykładnię systemową oraz wykładnię funkcjonalną (Stefański 2011, s. 497–512). Niezbędne jest także zwrócenie uwagi na treść art. 5 § 2 k.pk., zgodnie z którym nie dające się usunąć wątpliwości należy tłumaczyć na korzyść sprawcy, z tym zastrzeżeniem, że dopiero wtedy, gdy zostaną wykorzystane wszystkie właściwe reguły interpretacyjne (Kurowski 2020, s. 62).

Należy także zauważyć, że w art. 299 § 1 kodeksu karnego brak jest jakiegokolwiek ograniczenia do kategorii czynów zabronionych, czyli tzw. „czynów bazowych", z którymi powiązane są korzyści będące przedmiotem czynności wskazanych w art. 299 § 1 kodeksu karnego. Kategoria 22 rodzajów przestępstw dotyczy głównie przestępstw kryminalnych, nie obejmuje, poza przestępstwami podatkowymi oraz związanymi z wykorzystaniem informacji wewnętrznych i manipulacji na rynku, wielu przestępstw przeciwko obrotowi gospodarczemu oraz obrotowi cywilnemu, zamieszczonych w rozdziale XXXVI polskiego kodeksu karnego, przykładowo przestępstw przeciwko wierzycielom. Tylko udaremnienie lub ograniczenie zaspokojenia wierzycieli z art. 300 § 3 k.k. wchodziłoby do tej grupy, z uwagi na zagrożenie 6 miesięcy do 8 lat pozbawienia wolności. W tym zakresie mogą wystąpić poważne różnice w systemach karnych poszczególnych państw, a to będzie prowadziło do rozbieżnej praktyki organów ścigania oraz wymiaru sprawiedliwości. Jeśli chodzi o sprawców przestępstw prania pieniędzy, to będą oni poszukiwali takich miejsc, w których uregulowania będą dla nich korzystniejsze. Takie różnice

mogą zniweczyć osiągnięcie zamierzonego celu w postaci pozbawienia sprawców przestępstw owoców, powstałych z ich popełnienia.

Istotne problemy może także sprawiać dostosowanie się do zapisów art. 5 ust. 2 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r., przewidującego kary dla osób fizycznych, zgodnie z którym: „[p]aństwa członkowskie podejmują środki niezbędne do zapewnienia, aby przestępstwa, o których mowa w art. 3 ust. 1 i 5, podlegały karze w maksymalnym wymiarze co najmniej czterech lat pozbawienia wolności". Podkreślenia wymaga to, że mowa jest o maksymalnym wymiarze ustawowym kary co najmniej 4 lat pozbawienia wolności. Opisane w art. 3 ust. 1 i 5 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r. zachowania są formami prania brudnych pieniędzy z art. 299 § 1 k.k., gdzie maksymalne zagrożenie wynosi 8 lat pozbawienia wolności. Zwraca na to uwagę także B. Piątkowska oraz K. Skelnik, wskazując, że maksymalnie może być kara 4 lat pozbawienia wolności (Piątkowska i Skelnik 2022, s. 203). Autorzy dochodzą do wniosku, że jest to zgodne z zagrożeniem z art. 299 § 1 k.k., z czym nie można się do końca zgodzić (Piątkowska i Skelnik 2022, s. 208). Określenie: *czyn taki zagrożony był maksymalną karą pozbawienia wolności w wymiarze co najmniej 4 lat* nie jest jednoznaczne i nie wskazuje, o którą dolną czy górną granicę zagrożenia ustawowego chodzi. Gdyby przyjąć, że chodzi o górną granicę kary pozbawienia wolności w wymiarze co najmniej 4 lat, to taka regulacja mogłaby być uznana za zgodną z polską, ponieważ w art. 299 § 1 k.k. jest mowa o ustawowym zagrożeniu w wymiarze od 6 miesięcy do 8 lat pozbawienia wolności. W przeciwnym wypadku powstałaby sprzeczność z polską regulacją, ponieważ tylko w przypadku przygotowania do przestępstwa prania brudnych pieniędzy zagrożenie ustawowe wynosi 3 lata (art. 299 § 6a kodeksu karnego). Należy uznać to tłumaczenie za niezbyt szczęśliwe i przyjąć – na podstawie artykułu 1 Dyrektywy, że chodzi o ustanowienie minimalnych kar w dziedzinie prania pieniędzy. W przeciwnym wypadku doszłoby do absurdu.

Trzeba jeszcze dodać, że zgodnie z art. 4 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r. Państwa członkowskie zobowiązały się podjąć niezbędne środki, aby pomocnictwo, podżeganie i usiłowanie popełnienia przestępstw podlegały karze jako przestępstwa. Już w odniesieniu do pomocnictwa z art. 299 § 6a kodeksu karnego widoczna jest sprzeczność z art. 4 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r. Wymóg Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r. w pozostałych wypadkach nie wydaje się trudny do spełnienia, jeśli zważyć, że tendencja w polskiej polityce karania zmierza w kierunku zwiększenia ustawowego zagrożenia karą pozbawienia wolności, niż jej obniżania. Może także dojść do takiej sytuacji, kiedy przestępstwo prania pieniędzy będzie w zakresie zagrożenia ustawowego nieadekwatne do przestępstwa bazowego i to w znacznym zakresie.

Wydaje się, że brak jest także spójności art. 6 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r. z art. 258 k.k., ponieważ popełnienie przestępstwa: *działając w zorganizowanej grupie przestępczej* daje podstawę do wymierzenia kary tak jak osobie odpowiadającej w warunkach recydywy szczególnej wielokrotnej, ale, na podstawie art. 65 § 2 kodeksu karnego, z wyjątkiem zaostrzenia kary. W polskim

prawie karnym działanie w zorganizowanej grupie przestępczej jest formą udziału w tej grupie, a to stanowi odrębny czyn zabroniony, a nie okoliczność obciążającą. Na gruncie polskiego prawa nie jest także możliwe przyjęcie, że branie udziału w zorganizowanej grupie przestępczej zostanie uznane i za czyn zabroniony i jednocześnie za okoliczność obciążającą.

Drugą okolicznością obciążającą, zgodnie z art. 6 ust. 1 Dyrektywy VI AML, jest popełnienie czynu zabronionego prania pieniędzy przez sprawce, który jest podmiotem zobowiązanym w rozumieniu art. 2 Dyrektywy 2015/849 i jednocześnie do prania doszło podczas prowadzonej działalności zawodowej. Należy zwrócić uwagę, że przy użyciu spójnika „*i*" znacznie ogranicza się możliwości uznania za okoliczności obciążające. Gdyby taki warunek minimalny przyjmować, to należałoby go wprowadzić do art. 53 § 2 k.k. jako nową okoliczność obciążającą w postaci popełnienia przestępstwa: *podczas prowadzenia swojej działalności zawodowej i przez podmiot zobowiązany*. Pierwsza z okoliczności obciążających nie jest tożsama z uczynieniem sobie stałego źródła dochodu z popełnienia przestępstwa, występującego w polskim kodeksie karnym, ponieważ oba pojęcia nie mają tożsamego zakresu. Z jednej strony możliwe jest uczynienie sobie stałego źródła dochodu z działalności, która nie jest działalnością zawodową, a z drugiej strony działalność zawodowa nie musi przynosić stałego źródła dochodu.

Wprawdzie powołany art. 53 § 2 k.k. zawiera określenie *w szczególności*, które czyni katalog otwartym i możliwe jest uznanie przez Sąd popełnienie przestępstwa prania pieniędzy w ramach prowadzonej działalności zawodowej, jako okoliczności obciążającej, ale lepiej byłoby, gdyby ta okoliczność, wskazana w VI Dyrektywie, była wpisana do katalogu z art. 53 § 2 k.k.

Należałoby także rozważyć, czy pojęcie działalności zawodowej z VI Dyrektywy obejmuje działalność gospodarczą i na odwrót. Takie samo stanowisko co do poszerzenia katalogu okoliczności branych pod uwagę przy wymiarze kar zajęli W. Majkowski, M. Sawczuk, D. Muca, wskazując na konieczność zmiany art. 53 § 2 k.k. (Majkowski, Sawczuk i Muca 2021, s. 1012).

Zdaniem Autorki niniejszego artykułu, polski ustawodawca winien rozważyć także wpisanie do dyrektyw wymiaru kary z art. 53 § 2 k.k. jako okoliczności obciążającej „popełnienie przestępstwa z wykorzystaniem Internetu lub innych narzędzi komunikacji". Uzasadnieniem dla takiego stanowiska jest to, że skutkiem wykorzystania Internetu lub innych środków komunikacji jest szybsze komunikowanie się, szybsze dokonywanie transakcji i utrudnienia z zabezpieczeniem środków pieniężnych, które następnie stają się przedmiotem prania pieniędzy. W konsekwencji dochodzi do pokrzywdzenia znacznych ilości pokrzywdzonych z bardzo ograniczonymi widokami na możliwość zabezpieczenia środków do orzeczenia obowiązku naprawienia szkody.

Należałoby także wprowadzić zmiany w art. 9 ustawy z 28.10.2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Ustawa z 28.10.2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary – Dz.U. 2023, poz. 659), ponieważ przy odpowiedzialności podmio-

tu zbiorowego za przestępstwo prania brudnych pieniędzy nie przewidziano tak szerokiego zakresu środków jakie mogą być zastosowane wobec osób prawnych. W art. 8 omawianej Dyrektywy wskazane są jako kary chociażby czasowe lub stałe odcięcie od koncesji, objęcie nadzorem sądowym, sądowy nakaz likwidacji, czasowe lub stałe zamknięcie zakładów wykorzystywanych do popełnienia przestępstwa, których to środków karnych brak w polskiej ustawie z dnia 28 października 2002 roku, dotyczącej odpowiedzialności podmiotów zbiorowych (inaczej Golonka 2021, s. 42). Problematyczne byłoby, na gruncie polskiego kodeksu karnego, określenie czasu trwania tych środków karnych tylko na podstawie samej Dyrektywy, chociażby z tego względu, że nie został wskazany czas, na jaki mogą być orzeczone. Brak ten uniemożliwia zastosowanie Dyrektywy wprost, co oznacza, że winna być przeprowadzona nowelizacja ustawy o podmiotach zbiorowych.

Na gruncie polskiego prawa problematyczne jest także doprowadzenie do odpowiedzialności podmiotu zbiorowego, ponieważ w pierwszej kolejności należy doprowadzić do uzyskania prawomocnego wyroku skazującego do osoby fizycznej, a także podjęcia decyzji przez Sąd wskazanych w art. 4 powołanej ustawy. Taki warunek nie został wskazany w art. 7 ust. 1 VI Dyrektywy, nakazujący podjęcie państwom członkowskim niezbędnych środków do pociągnięcia osób prawnych za przestępstwa wskazane w art. 3 ust. 1 i 5 i art. 4 VI Dyrektywy, w celu przysporzenia tym podmiotom zbiorowym korzyści. Wprawdzie w prawie polskim dopuszczona jest wtórna odpowiedzialność podmiotu zbiorowego, ale wymóg uprzedniego prawomocnego skazania osoby fizycznej i możliwości prawnego oraz faktycznego zakończenia działalności przez podmioty zbiorowe utrudniają osiągnięcie minimalnego warunku pociągania do odpowiedzialności karnej podmioty zbiorowe.

Rozważenia wymaga także wprowadzenie do art. 299 k.k. nieumyślnej formy prania pieniędzy, a to dzięki treści pkt 13 preambuły VI Dyrektywy. Odwołując się do wykładni historycznej należy wskazać, że wprowadzenie przestępstwa prania pieniędzy do prawa polskiego było wynikiem niemożności wykorzystania, przy różnego rodzaju przekształceniach przedmiotu czynu zabronionego w korzyści majątkowe, przepisów dotyczących karania za paserstwo. Uniemożliwiał to opis czynności czasownikowych realizowanych przez sprawcę paserstwa oraz zakaz pociągania do odpowiedzialności za paserstwo sprawcy czynu uprzedniego. Jednak w poprzednim kodeksie karnym (art. 216 k.k.), jak i obecnym przewidziany został typ nieumyślny paserstwa (Dąbrowska-Kardas i Kardas 2016, s. 455), gdzie rozszerzenie karalności dotyczyło wykazania, że sprawca: „na podstawie towarzyszących okoliczności powinien i mógł przypuszczać, że rzecz została uzyskana za pomocą czynu zabronionego". Polski ustawodawca w art. 299 k.k. nie przewiduje typu nieumyślnego, co znacznie rozszerzyłoby możliwości zastosowania w/w przepisu.

Dodatkowo należy wskazać, że w przepisach polskiej procedury karnej winien został wprowadzony obowiązek, który nakazywałby poinformowanie Komisji, zgodnie z art. 10 ust. 2 Dyrektywy o rozszerzeniu jurysdykcji poza własne terytorium, jeżeli przestępstwo prania zostało popełnione poza terytorium kraju, a jednocześnie sprawca ma zwykłe miejsce pobytu lub pobytu lub przestępstwo zostało po-

pełnione na szkodę osoby prawnej mającej swoją siedzibę na terytorium kraju, który chce rozszerzyć jurysdykcję.

W polskiej procedurze jest tylko obowiązek powiadomienia zawiadamiającego o wszczęciu postępowania, ale jest to inny rodzaj obowiązku, nałożonego na organ w innym etapie postępowania.

Komisja nie jest zawiadamiającym. Brak takiego obowiązku w polskiej procedurze karnej może doprowadzić do zaniechania wykonania tego obowiązku.

Należy nadmienić, że ten obowiązek winien być doprecyzowany poprzez wskazanie zobowiązanego, czasu powiadomienia, a także formy powiadomienia (czy ma się odbywać za pośrednictwem prokuratur, w których są zatrudnieni prokuratorzy zajmujący się obrotem prawnym z zagranicą, czy też obowiązek ten spoczywa na prokuraturze nadzorującej postępowanie. Winna być doprecyzowana kwestia ewentualnego obowiązku przetłumaczenia pisma.

4. Inne braki w zakresie niezbędnej regulacji

Należy wspomnieć o innych przeszkodach natury prawnej, które, z jednej strony, są związane z szybkim procesem globalizacji, również w zakresie przestępczości, a z drugiej strony, z brakiem odpowiednio podążających za tym procesem zmian legislacyjnych. Dotyczy to braku szybkiej i bezpośredniej współpracy organów ścigania z zagranicznymi bankami w zakresie ustalania stanu rachunku bankowego, co do którego zachodzi podejrzenie, że został wykorzystany do przestępstwa prania brudnych pieniędzy. Generalny Inspektor Informacji Finansowej na podstawie artykułu 104 ustawy z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (Ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu – t.j. Dz.U. 2021, poz. 1132), posiada kompetencje, aby zwrócić się do odpowiedniego organu w państwie wezwanym o poczynienie takich ustaleń, ale twierdzi, że tylko wtedy może korzystać z tych kompetencji, gdy sam złożył doniesienie (Patora 2020, s. 211–229). Tymczasem znaczna część czynów ujawniana jest w toku prowadzenia postępowania przygotowawczego, bez doniesienia GIIF. Prowadzi to do wniosku, że szybkie czynności związane z wykorzystaniem środków pieniężnych pochodzących z czynów zabronionych, a popełniane za pomocą zagranicznych instrumentów finansowych i przy wykorzystaniu zagranicznych banków, nie będą w praktyce możliwe. Istnieją wprawdzie instrumenty wskazane w Europejskim Nakazie Dochodzeniowym (Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z 3.04.2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych, Dz.U.UE.L.2014.130.1), czy też w kierowanych do innych państw wnioskach o pomoc prawną, ale, przy możliwości dokonywania operacji bankowych za pomocą bankowości internetowej, są one dalece niewystarczające. Przykładowo, należy wskazać, że dokumenty dotyczące wykonania postanowienia o zabezpieczeniu majątkowym muszą być chociażby przetłumaczone, co daje przewagę czasową do wykonania czynności związanych z transferem środków po-

chodzących z przestępstwa, aby nie zostały zajęte. Wydaje się, że jest to sprzeczne z art. 11 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r., który nakłada na państwa członkowskie obowiązek podjęcia niezbędnych środków celem zapewnienia skutecznych narzędzi, stosowanych w postępowaniach przygotowawczych w walce z przestępczością zorganizowaną lub innymi poważnymi przestępstwami (Dyrektywa Parlamentu Europejskiego i Rady z 23.10.2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych – Dziennik Urzędowy Unii Europejskiej z 12.11.2018 r., L 284/22).

Kolejnym zagadnieniem, które należy podnieść i odnieść jako brak wymaganych regulacji w zakresie związanym z przestępstwem prania „brudnych" pieniędzy, jest brak odpowiednich przepisów, które dałyby możliwości odroczenia doręczenia postanowienia o zabezpieczeniu majątkowym w polskiej procedurze karnej. Postanowienie to wydawane jest w razie potrzeby zabezpieczenia środków, w tym do zasądzenia środka kompensacyjnego, zwrotu pokrzywdzonemu korzyści majątkowej, jaką sprawca osiągnął z popełnienia przestępstwa albo jej równowartości. Powołany przepis służy rzeczywistemu pozbawieniu sprawców korzyści, jakie osiągnęli z popełnienia przestępstwa i zwrotu ich pokrzywdzonym. Zabezpieczenie może nastąpić na mieniu oskarżonego lub na mieniu wskazanym w art. 45 § 2 kodeksu karnego, czyli mieniu, które sprawca objął we władanie lub do którego uzyskał jakikolwiek tytuł prawny w ciągu 5 lat przed popełnieniem przestępstwa, chyba że sprawca lub inna osoba wykaże dowód przeciwny. Zgodnie z treścią art. 291 kodeksu postępowania karnego konieczne jest wydanie postanowienia o zabezpieczeniu majątkowym na mieniu podejrzanego między innymi w celu naprawienia szkody wyrządzonej przestępstwem. W przypadku obrotu prawnego z zagranicą niezbędne jest do jego realizacji dokonanie tłumaczenia tegoż dokumentu, a także innych dokumentów, które są związane z wyekspediowaniem wniosku o pomoc prawną lub Europejskiego Nakazu Dochodzeniowego. Polski ustawodawca nie przewidział możliwości odroczenia doręczenia postanowienia o zabezpieczeniu majątkowym na mieniu, które podejrzany, przebywający w Polsce, posiada za granicą. Brak takiej możliwości niweczy wszelkie wysiłki, które są podejmowane w celu zabezpieczenia mienia, które pochodzi z przestępstwa. Skoro możliwość odroczenia doręczenia postanowienia na czas oznaczony, nie później niż do czasu prawomocnego zakończenia postępowania, jest przewidziana w art. 218 § 2 kodeksu postępowania karnego (Ustawa z 6.06.1997 r. Kodeks postępowania karnego – Dz.U. 2021, poz. 534), w odniesieniu do korespondencji, to należy rozważyć wprowadzenie podobnego przepisu w odniesieniu do postanowienia o zabezpieczeniu majątkowym, również na czas oznaczony, nie później niż do wykonania postanowienia o zabezpieczeniu majątkowym. Na podstawie powołanego już art. 11 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r. podjęcie takich środków wydaje się jak najbardziej uzasadnione. Wskazane wyżej rozwiązanie winno przyczynić się do spełnienia wymogu wskazanego w art. 9 Dyrektywy Parlamentu Europejskiego i Rady z 23.10.2018 r., który nakłada na państwa członkowskie obowiązek niezbędnych działań do zabezpieczenia oraz konfiskaty korzyści pochodzących z przestępstw prania „brudnych" pieniędzy. Wymóg ten w polskim prawie będzie coraz trudniej-

szy do spełnienia, szczególnie, gdy SN w uchwale z 13.10.2021 r., I KZP 1/21, wskazał, że art. 86 ust. 13 ustawy z 1.03.2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu musi być interpretowany w sposób ścisły, a środki zgromadzone na rachunkach bankowych nie mają cech dowodu rzeczowego (Uchwała SN z 13.10.2021 r., I KZP 1/21, OSNK 2021/11-12/42, Lex nr 3239937). Wprawdzie ustawodawca dodał art. 236b kodeksu postępowania karnego (Ustawa z 17.12.2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości – Dz.U. 2021, poz. 2447), który daje możliwość uznania za dowody rzeczowe środków zgromadzonych na rachunku bankowym, jeśli zostały zatrzymane jako dowody rzeczowe, ale nadal pozostaje problem gwarancyjnych funkcji tego rozwiązania, z punktu widzenia czasu przechowywania takich środków jako dowodu rzeczowego. Problem jest trudny, ponieważ, z jednej strony, chodzi o szybkie zabezpieczenie pieniędzy na rachunku bankowym, a z drugiej strony, czas ustaleń może się znacznie wydłużyć, szczególnie jeśli zachodzi konieczność uzyskania międzynarodowych pomocy prawnych.

Dyrektywa Parlamentu Europejskiego i Rady z 23.10.2018 r. przewiduje minimalne wymagania w zakresie karalności przestępstwa prania pieniędzy i każde państwo może w zakresie ścigania tego typu czynów zabronionych pójść znacznie dalej, ale przy transgranicznym charakterze prania pieniędzy, nie dające się usunąć wątpliwości w ustawodawstwach, zarówno w prawie karnym materialnym, jak i procesowym, będą musiały być interpretowane na korzyść potencjalnego sprawcy (art. 5 § 2 kodeksu karnego). To oznacza, że konieczne będzie badanie obowiązującego prawa w miejscu popełnienia czynu zabronionego, które będzie znajdowało się także poza granicami Polski. Przyjęcie w Polsce, że każdy czyn zabroniony będzie mógł stanowić czyn bazowy prania pieniędzy, nie oznacza, że takie podejście przyjęte zostanie w innych krajach. Dlatego konieczne będzie stosowanie zasady podwójnej karalności, wskazanej w art. 111 § 1 kodeksu karnego.

Podsumowanie

Proces ujednolicania prawa w zakresie prania brudnych pieniędzy z prawem krajowym jest niezwykle trudny i skomplikowany. Niespójność występuje zarówno na podstawie przepisów prawa materialnego, jak i procedury. Dotyczy to także prawa krajowego, materialnego oraz prawa procesowego, które nie są dostosowane do zmieniających się możliwości w zakresie rozporządzania mieniem, które pochodzi z przestępstwa. Wydaje się, że dla skutecznej walki z praniem pieniędzy niezbędne są bardziej spójne systemy prawne poszczególnych państw i zagwarantowanie bezpośredniej współpracy organów ścigania i banków. Wprowadzenie rozwiązań wskazanych w najnowszej Dyrektywie może skutkować ograniczeniem w zakresie karnych przepisów dotyczących przestępstw prania brudnych pieniędzy, w porównaniu do krajowych regulacji, co będzie miało znaczenie przy transgranicznym praniu pieniędzy. Dlatego też wypracowanie minimalnych wspólnych rozwiązań jest sukcesem, ale w praktyce może mieć ograniczony wymiar.

Bibliografia

Błachnio A. (2024), [w:] J. Majewski (red.), *Kodeks karny. Komentarz*, WKP, teza 15.

Buchała K., Kardas P., Majewski J., Wróbel W. (1995), *Komentarz do ustawy o ochronie obrotu gospodarczego*, Warszawa.

Chatee S. (2022), *Financial Crime in 2021 – Brexit and the 6th Anti Money Laundering Directive*, https://sqa-consulting.com/financial-crime-in-2021-brexit-and-the-6th-anti-money-laundering-directive/ (dostęp 2.07.2022).

Czepukojć M. (2017), *Problematyka środków pieniężnych zgromadzonych na koncie bankowym w kontekście przedmiotu przestępstwa z art. 299 k.k. Glosa do uchwały SN z dnia 24 czerwca 2015 r., I KZP 5/15*, Glosa nr 1.

Dąbrowska-Kardas M., Kardas P. (2016), [w:] A. Zoll (red.), *Kodeks karny. Część szczególna. Tom III. Komentarz do art. 278–363*, Warszawa.

Duży J. (2010), *Pojęcie korzyści związanych z popełnieniem czynu zabronionego*, Glosa do postanowienia SN z 1.09.2010 r., V KK 43/10.

Gadecki B. (2023), [w:] B. Gadecki (red.), *Kodeks karny. Art. 1–316. Komentarz*, Warszawa.

Gałązka M. (2024), [w:] A. Grześkowiak, K. Wiak (red.), *Kodeks karny. Komentarz*. Warszawa.

Giezek J. (red.) (2021), *Kodeks karny. Część szczególna. Komentarz*, WKP, teza 35.

Giezek J. (2013), *Glosa do uchwały SN z 18.12.2013 r.*, I KZP 19/13, teza nr 4.

Gilmore W.C. (1999), *Brudne Pieniądze. Metody Przeciwdziałania Praniu Pieniędzy*, Warszawa.

Golonka A. (2021), *Polskie regulacje karne wobec „szóstej" dyrektywy anti-money laudering*, Ius Novum nr 1.

Górniok O. (2000), *Przestępstwa gospodarcze Rozdział XXXVI i XXXVII Kodeksu karnego. Komentarz*, Warszawa.

Górniok O. (red.), (2003), *Prawo karne gospodarcze*, tom 10, Warszawa.

Kurowski M. (2020), [w:] D. Świecki, *Kodeks postępowania karnego*, Komentarz, tom I, Art. 1–424, Warszawa.

Lizak R. (2018), *Pranie pieniędzy w prawie polskim na tle europejskim, międzynarodowym i amerykańskim*, Warszawa.

Majkowski W., Sawczuk M., Muca D. (2021), *Dyrektywa VI AML a obecnie obowiązujące polskie prawo krajowe*, Monitor Prawniczy nr 19.

Michalska-Warias A. (2016), *Glosa do postanowienia z dnia 12 stycznia 2015 r., III KK 247/14*, WPP nr 1.

Oczkowski T. (2023), [w:] V. Konarska-Wrzosek (red.), *Kodeks karny. Komentarz*, wyd. IV, WKP, teza 7.

Patora K. (2020), *Współpraca prokuratora z Generalnym Inspektorem Informacji Finansowej w zakresie spraw karnych dotyczących przestępstw z art. 299 k.k.*, 2020, „Prokuratura i Prawo", nr 7–8.

Piątkowska B., Skelnik K. (2022), *Rozwiązania obowiązujące w polskim systemie karnym w instytucjach obowiązanych w kontekście dyrektyw anti-money laundering*, Probacja nr 4.

Pływaczewski E. (1993), *Pranie brudnych pieniędzy. Możliwości przeciwdziałania z uwzględnieniem roli systemu bankowego*, Toruń.

Potulski J. (2023), [w:] R.A. Stefański (red.), *Kodeks karny. Komentarz*. Warszawa/Legalis.

Stefański R. (2011), [w:] T. Bojarski (red.), *Źródła prawa karnego*, Warszawa.

Wahl T. (2021), *AML Package III: 6th AML Directive Proposed*, https://eucrim.eu/news/aml-package-iii-6th-aml-directive-proposed/ (dostęp 14.03.2022).

Ward D. (2021), *How new rules on financial crime will impact the EU AML regime*, https://www-ey-com.translate.goog/en_sy/financial-services-emeia/how-new-rules-on-financial-crime-will-impact-the-eu-aml-regime?_x_tr_sl=en&_x_tr_tl=pl&_x_tr_hl=pl&_x_tr_pto=-op,sc (dostęp 2.07.2022).

Wąsowski K. (2001), *Pranie brudnych pieniędzy*, „Materiały i Studia" NBP, z. 121, Warszawa.

Wójcik J.W. (2002), *Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Warszawa.

Wróbel T. (2012), *Zakres tzw. źródłowych czynów zabronionych – przestępstwo prania brudnych pieniędzy w kontekście regulacji międzynarodowych,* Czasopismo Prawa Karnego i Nauk Penalnych, nr 4.

Zawłocki R., Gałęski M. (2024), [w:] M. Królikowski, R. Zawłocki (red.), *Kodeks karny. Komentarz*, Warszawa/Legalis.

Zoll A. (2016), *Kodeks karny. Część szczególna*, tom III, Warszawa.

Orzeczenia sądowe

Uchwała SN z 4.04.2005 r., I KZP 7/05, OSNKW 2005/5/44.

Postanowienie SA w Katowicach z 15.07.2009 r., II AKz 417/09, KZS 2010/11/55, OSA 2010/7/3-10).

Wyrok SA w Krakowie z 28.10.2009 r., II AKa 184/09, KZS 2009/12/61.

Wyrok SA w Łodzi z 13.12.2012 r., II AKa 198/12; KZS 2014/11/53/.

Uchwała 7 Sędziów SN (zasada prawna) z 18.12.2013 r., I KZP 19/13, OSNKW 2014, Nr 1, poz. 1.

Postanowienie SN z 12.01.2015 r., III KK 247/14, Lex nr 1622321.

Postanowienie SN z 30.11.2017 roku, IV KK 272/17, Lex nr 2434470.

Uchwała SN z 13.10.2021 r., I KZP 1/21, OSNK 2021/11-12/42, Lex nr 3239937.

Akty prawne

Bank Secrecy Act of 1970 r., 84 Stat. 1114.

Committee of Ministers of the Council of Europe, *Recommendation No. R (80) 10 on measures against the transfer and the safekeeping of funds of criminal origin*, 27.06.1980, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f6231 (dostęp 2.01.2022).

Ustawa z 20.05.1971 r. Kodeks wykroczeń – Dz.U. 2021, poz. 2008.

Konwencja Narodów Zjednoczonych o zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi, sporządzona w Wiedniu 20.12.1988 r., Dz.U. 1995 Nr 15, poz. 69 z 20.02.1995.

Dyrektywa Rady 91/308/EWG z 10.06.1991 r. w sprawie uniemożliwienia korzystania z systemu finansowego w celu prania pieniędzy – Dz.U.UE L z 28.06.1991 r., Dz.U.UE.L.1991.166.77.

Zarządzenie nr 16/92 Prezesa Narodowego Banku Polskiego z 1.10.1992 r. w sprawie zasad postępowania banków w razie ujawnienia okoliczności wskazujących na lokowanie w banku środków pieniężnych lub innych wartości majątkowych pochodzących lub mających związek z przestępstwem oraz przy dokonywaniu wpłat gotówkowych przekraczających określoną kwotę Dz.Urz. NBP z 2.10.1992 r., 20.9.1992.

Ustawa z 12.10.1994 r. o ochronie obrotu gospodarczego i zmianie niektórych przepisów prawa karnego – Dz.U. Nr 126, poz. 615.

Ustawa z 6.06.1997 r. Kodeks karny – t.j. Dz.U. 2021, poz. 2345.

Ustawa z 6.06.1997 r. Kodeks postępowania karnego – Dz.U. 2021, poz. 534.

Ustawa z 10.09.1999 r. Kodeks karny skarbowy – t.j. Dz.U. 2021, poz. 408.

Konwencja Narodów Zjednoczonych z 15.11.2000 r. przeciwko międzynarodowej przestępczości zorganizowanej – Dz.U. 2005 Nr 18, poz. 158 z 31.01.2005.

Ustawa z 16.11.2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – Dz.U. 2017, poz. 1049.

Konwencja Nr 141 o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa, ratyfikowana przez Polskę w 2000 r. (Dz.U. 2003 Nr 46, poz. 394).

http://conventions.coe.int/Treaty/en/Treaties/Html/141.html (dostęp 1.01.2022).

Ustawa z 28.10.2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary – Dz.U. 2020, poz. 358.

Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzona w Warszawie 16.05.2005 r. – Dz.U. 2008 Nr 165, poz. 1028.

Ustawa z 25.06.2009 r. o zmianie ustawy o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu oraz o zmianie niektórych innych ustaw – Dz.U. 2009 Nr 166, poz. 1317.

Dyrektywa Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem – Dz.U.UE.L.2007.332.103 z dnia 18.12.2007.

Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z 3.04.2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych, Dz.U.UE.L.2014.130.1.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z 20.05.2015 r. w sprawie zapobiegania wykorzystywaniu 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.U.UE L z 5.06.2015 r., Dz.U.UE.L.2015.141.73 ze zm.

Ustawa z 09.10.2015 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw – Dz.U. 2015, poz. 1855.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1673 z dnia 23.10.2018 r. w sprawie zwalczania prania pieniędzy za pomocą środków prawnokarnych Dz.U.UE.L.2018.284.22 z dnia 12.11.2018.

Ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – Dz.U. 2023, poz. 1124.

Ustawa z 17.12.2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości – Dz.U. 2021, poz. 2447.

DOI: 10.26354/bb.4.1.94.2024

Adam Karmoliński*
ORCID: 0009-0002-9360-4294
karmolinski.adam@gmail.com

Adrian Rycerski**
ORCID: 0000-0002-4673-0450
rycerski.adrian@gmail.com

Możliwość wymiany informacji w ramach zrzeszenia banków spółdzielczych na gruncie przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

Streszczenie

Celem artykułu jest przybliżenie wątpliwości prawnych w zakresie funkcjonowania zrzeszeń banków spółdzielczych pod kątem wykonywania przez nie obowiązków dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Prezentowane w artykule wątpliwości prawne znacznie utrudniają, lub nawet uniemożliwiają, współdziałanie zrzeszonym bankom spółdzielczym w zakresie stosowania przepisów AML/CFT. Opisywane wątpliwości stwarzają bowiem istotne ryzyko po stronie zrzeszeń banków spółdzielczych, które bez ingerencji prawodawcy będzie niezwykle trudno wyeliminować. Artykuł przedstawia również podstawy prawne działań zrzeszeń banków spółdzielczych, z uwzględnieniem problematyki przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Autorzy prezentują postulaty *de lege ferenda*.

Słowa kluczowe: bank spółdzielczy, zrzeszenie banków spółdzielczych, przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu, czynności bankowe, prawo bankowe

Kody JEL: K20, K22, K23

* Adam Karmoliński – OIRP w Warszawie, aplikant radcowski.
** Adrian Rycerski – Uniwersytet SWPS w Poznaniu, adwokat.

Possibility to exchange information within an association of cooperative banks on the grounds of anti-money laundering and counter-terrorist financing regulations

Abstract

The purpose of this article is to highlight the legal uncertainties in the functioning of cooperative banking associations with regard to the implementation of the obligations relating to the prevention of money laundering and the financing of terrorism. The legal doubts presented in the article make it very difficult, if not impossible, for cooperative banks to cooperate in the implementation of AML/CFT regulations. The uncertainties mentioned above generate significant risks on the side of cooperative bank associations, which will be extremely difficult to eliminate without legislative intervention. The article also presents the legal basis for the activities of cooperative banking associations, taking into account AML/CFT issues. The authors present *de lege ferenda* postulates.

Keywords: cooperative bank, association of cooperative banks, anti-money laundering and countering the financing of terrorism, banking activities, banking law

JEL Codes: K20, K22, K23

Wstęp

Celem niniejszego artykułu jest przybliżenie wątpliwości prawnych w zakresie funkcjonowania zrzeszeń banków spółdzielczych pod kątem wykonywania przez nie obowiązków dotyczących przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Artykuł przedstawia potencjalne możliwości oraz jednocześnie istotne ograniczenia w stosowaniu przepisów TerroryzmU przez banki należące do zrzeszeń banków spółdzielczych w zakresie współpracy pomiędzy tymi podmiotami. Artykuł skupia się bowiem na obowiązku nałożonym na instytucje obowiązane (którymi są również banki spółdzielcze) w postaci zachowania w tajemnicy przekazywanych informacji, wyrażony w art. 54 ust. 1 TerroryzmU[1].

Niniejsza praca dotyczy doniosłego problemu jakim jest wątpliwość stosowania przez zrzeszenia banków spółdzielczych określonych przepisów TerroryzmU właściwych dla grup kapitałowych. Z tego powodu autorzy tekstu pokazują podobieństwa pomiędzy zrzeszeniem a grupą kapitałową, które mogłyby zostać wykorzystane przy wykładni funkcjonalnej TerroryzmU. Jednym z zadań artykułu jest ponadto zaprezentowanie postulatów *de lege ferenda* dotyczących oczekiwanych zmian w zakresie niedopatrzeń ustawowych wobec banków spółdzielczych oraz zrzeszeń banków spółdzielczych chcących wypełniać swoje obowiązki zgodnie z przepisami i celami TerroryzmU.

[1] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r. poz. 723 ze zm.).

1. Sytuacja banków spółdzielczych

1.1. Zrzeszenie banków spółdzielczych – podstawowe pojęcia

Poprzez zrzeszenie należy rozumieć zrzeszenie działające na podstawie BankSpółU[2], utworzone przez bank lub banki spółdzielcze i bank zrzeszający (art. 2 pkt 3 BankSpółU). Bankiem spółdzielczym jest bank funkcjonujący w formie spółdzielni, do którego w zakresie nieuregulowanym w BankSpółU oraz w PrBank[3] stosuje się przepisy ustawy z dnia 16 września 1982 r. – Prawo spółdzielcze (art. 2 pkt 1 BankSpółU). Z kolei przez bank zrzeszający należy rozumieć bank w formie spółki akcyjnej, utworzony przez banki spółdzielcze, jeżeli bank ten zrzesza co najmniej jeden bank spółdzielczy na zasadach zrzeszenia oraz posiada kapitał założycielski wynoszący co najmniej czterokrotność kwoty wskazanej w art. 32 ust. 1 PrBank (na dzień sporządzenia artykułu jest to równowartość kwoty 5.000.000,00 euro) lub jej dwukrotność, jeżeli działalność banku zrzeszającego ogranicza się wyłącznie do świadczenia usług na rzecz zrzeszonych banków (tzw. apeksowy bank zrzeszający)[4] (art. 2 pkt 2 BankSpółU).

1.2. Zrzeszenie banków spółdzielczych w ujęciu funkcjonalnym

Zrzeszenie banków spółdzielczych w ujęciu funkcjonalnym stanowi jeden organizm gospodarczy o specyficznych cechach i systemie wzajemnego wspierania się. Ową specyfikę bardzo dobrze uwidacznia relacja własności zachodząca pomiędzy uczestnikami zrzeszenia (Szczęśniak 2019). Bank zrzeszający, stojący niejako na czele całego zrzeszenia, w dodatku pełniący funkcję podmiotu zrzeszającego, jest własnością banków spółdzielczych, bowiem to właśnie banki spółdzielcze muszą posiadać co najmniej jedną akcję banku zrzeszającego (Zalcewicz 2009). Struktura własnościowa oraz sposób zaangażowania kapitałowego w zrzeszeniu banków spółdzielczych cechuje się zatem odmiennością w porównaniu do grup kapitałowych funkcjonujących w obrocie gospodarczym[5], w których to podmiot stojący na ich czele (podmiot dominujący) jest właścicielem pozostałych podmiotów wchodzących w skład grupy (podmiotów zależnych). W przypadku grup kapitałowych rola wspierająca podmiotu dominującego wynika przede wszystkim ze stosunku właścicielstwa, natomiast w przypadku zrzeszenia banków spółdzielczych jej źró-

[2] Ustawa z dnia 7 grudnia 200 r. o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających (Dz.U. 2000 Nr 119, poz. 1252 ze zm.).

[3] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. 1997 Nr 140, poz. 939 ze zm.).

[4] W niniejszym artykule nie jest poruszana problematyka szczególnego rodzaju zrzeszenia, jakim jest zrzeszenie zintegrowane (art. 2 pkt 7 BankSpółU).

[5] Jako typowe grupy kapitałowe należy uznać takie grupy, w których wyróżnia się podmiot pełniący rolę spółki „matki", tj. spółki dominującej wobec innych podmiotów – spółek „córek", tj. spółek zależnych. Spółka dominująca, posiadając pakiet kontrolny w postaci akcji, bądź udziałów spółek zależnych, wywiera wpływ oraz decyduje o losach podmiotów należących do grupy.

dłem są uregulowania prawne stawiające bank zrzeszający w szczególnej roli (zob. np. art. 19 ust. 2 BankSpółU) (Bączyk 2020).

Co więcej, można się pokusić o stwierdzenie, że bank zrzeszający jeszcze intensywniej spaja zrzeszenie aniżeli czyni to podmiot dominujący w grupie kapitałowej. Bank zrzeszający ma szerokie uprawnienia do zarządzania czy prowadzenia spraw zrzeszenia, a także reprezentacji banków spółdzielczych w stosunkach zewnętrznych w sprawach wynikających z umowy zrzeszenia. Ponadto bank zrzeszający pełni funkcję swoistego inicjatora oraz organizatora zrzeszenia, tworząc swojego rodzaju formę konsolidacji organizacyjnej (Zalcewicz 2009). Zrzeszenia banków spółdzielczych powinny zatem korzystać z ułatwień, które przewidziane są dla grup kapitałowych. Przemawiają za tym nie tylko względy funkcjonalne (wskazane wyżej), ale także potrzeba podejmowania adekwatnych i skutecznych działań w zakresie AML/CFT[6]. Tymczasem wydaje się, że zarówno prawodawca unijny, jak i krajowy, nie dostrzegają potrzeb zrzeszenia, co zostanie rozwinięte w dalszej części niniejszego artykułu.

1.3. Znaczenie współpracy w zakresie wymiany informacji istotnych z perspektywy AML/CFT

W ramach prawidłowego oraz skutecznego wykonywania obowiązków związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu, podmioty finansowe (banki, firmy inwestycyjne czy instytucje płatnicze), jako instytucje obowiązane, mające w dodatku zagwarantować najwyższy standard ochrony interesów klientów przed jakimikolwiek działaniami oszukańczymi, powinny prowadzić szeroko zakrojone działania celem identyfikowania osób oraz transakcji o potencjalnie wyższym ryzyku prania pieniędzy i finansowania terroryzmu. W przypadku instytucji finansowych należących do jednej grupy kapitałowej wymiana informacji istotnych z perspektywy przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu jest możliwa na podstawie art. 54 ust. 2 pkt 2 TerroryzmU, który przewiduje, że podmioty wchodzące w skład tej samej grupy, pod warunkiem stosowania przez te jednostki ustanowionej w obrębie grupy strategii w zakresie ochrony danych oraz procedur dotyczących wymiany informacji do celów AML/CFT, nie mają obowiązku zachowania w tajemnicy informacji, o których mowa w art. 54 ust. 1 TerroryzmU.

Wychodząc naprzeciw takim założeniom, należałoby uznać, że instytucje finansowe, w tym banki spółdzielcze należące do zrzeszeń banków spółdzielczych, powinny dysponować odpowiednio podobnymi narzędziami ustawowymi, które umożliwiałyby sprawną wymianę informacji dotyczących podejmowanych działań w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Można w istocie wysnuć hipotezę, że na gruncie powyższych rozważań, zrzeszenie

[6] Anti-money laundering/combating the financing of terrorism – przeciwdziałanie praniu pieniędzy/finansowaniu terroryzmu.

banków spółdzielczych należałoby traktować jako jeden organizm gospodarczy, a wymiana wspomnianych informacji mogłaby odbywać się według uznania zaangażowanych podmiotów. Niemniej jednak działalność zrzeszeń banków spółdzielczych, polegająca na gromadzeniu, udostępnianiu i przekazywaniu konkretnych informacji związanych z analizami w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, doznaje istotnych ograniczeń.

1.4. Obowiązek zachowania tajemnicy

Zgodnie z art. 54 ust. 1 TerroryzmU instytucje obowiązane, ich pracownicy oraz inne osoby działające w imieniu i na rzecz instytucji obowiązanych zachowują w tajemnicy: (i) fakt przekazania GIIF[7] lub innym właściwym organom informacji określonych w rozdziałach 7 i 8 TerroryzmU (znajdują się tam przepisy wskazujące na obowiązki instytucji obowiązanych w zakresie odpowiednio przekazywania i gromadzenia informacji oraz wstrzymywania transakcji i blokowania rachunków); (ii) informacje o planowaniu wszczęcia oraz o prowadzeniu analizy dotyczącej prania pieniędzy lub finansowania terroryzmu.

Zakaz przekazywania osobom nieuprawnionym informacji o planowaniu wszczęcia oraz o prowadzeniu analizy dotyczącej prania pieniędzy lub finansowania terroryzmu naturalnie prowadzi do takich pojęć, jak: analiza finansowa, analiza operacyjna oraz analiza strategiczna, które zostały zdefiniowane odpowiednio w art. 2 ust. 2 pkt 1a–1c TerroryzmU. Analiza finansowa stanowi wynik analizy operacyjnej lub analizy strategicznej przeprowadzonej przez GIIF w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Analiza operacyjna jest metodą działania opartą na badaniu, przetwarzaniu i zestawianiu zgromadzonych informacji, polegającą na poszukiwaniu, identyfikowaniu i wskazywaniu powiązań między danymi uzyskanymi z różnych źródeł w celu wykrycia lub uprawdopodobnienia prania pieniędzy lub finansowania terroryzmu. Z kolei analiza strategiczna oznacza metodę działania opartą na badaniu, przetwarzaniu i zestawianiu zgromadzonych informacji, polegającą na poszukiwaniu, identyfikowaniu i wskazywaniu tendencji oraz schematów działania w zakresie prania pieniędzy lub finansowania terroryzmu.

Pomimo wprowadzenia definicji legalnych analizy finansowej, operacyjnej oraz strategicznej do TerroryzmU i powiązania tych czynności z działalnością wykonywaną przez GIIF (zgodnie z uzasadnieniem do projektu ustawy zmieniającej TerroryzmU), treść art. 54 ust. 1 pkt 2 TerroryzmU nadal nie została sprecyzowana w zakresie podmiotu, który planuje wszczęcie lub prowadzi analizę dotyczącą przeciwdziałania prania pieniędzy lub finansowania terroryzmu. Wykładnia językowa art. 54 ust. 1 pkt 2 TerroryzmU nie pozwala jednoznacznie stwierdzić, czy informacje o planowaniu wszczęcia oraz prowadzeniu analizy dotyczącej prania pieniędzy lub finansowania terroryzmu odnoszą się wyłącznie do czynności podejmowanych

[7] Generalny Inspektor Informacji Finansowej.

w tym zakresie przez GIIF, czy też obejmują czynności podejmowane przez instytucje obowiązane.

Powyższe oznacza, że proces polegający na gromadzeniu, udostępnianiu i przekazywaniu konkretnych informacji związanych z analizami w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, może (ale niekoniecznie musi) podlegać pod zakaz wymiany informacji, o którym mowa w art. 54 ust. 1 TerroryzmU.

1.5. Wyjątki od zakazu zachowania tajemnicy

Zakaz przewidziany w art. 54 ust. 1 TerroryzmU nie jest bezwzględny, a ustawodawca przewidział od niego cztery wyjątki. Zgodnie z art. 54 ust. 2 pkt 1–4 TerroryzmU, dozwolona jest wymiana informacji:

1) pomiędzy instytucjami kredytowymi i finansowymi z siedzibą w państwach członkowskich UE należącymi do tej samej grupy oraz pomiędzy tymi instytucjami a ich oddziałami i jednostkami zależnymi z większościowym udziałem tych instytucji mającymi siedzibę w państwie trzecim, wchodzącymi w skład grupy, pod warunkiem stosowania przez te podmioty strategii oraz zasad postępowania określonych w procedurze grupowej;
2) pomiędzy m.in. notariuszami, adwokatami, radcami prawnymi oraz osobami z państw trzecich, które podlegają takim samym wymogom jak w AMLD[8] lub równoważnym i wykonują swoje czynności zawodowe w ramach tej samej osoby prawnej lub w ramach struktury mającej wspólnego właściciela, wspólny zarząd lub wspólną kontrolę zgodności z przepisami z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, w skład której wchodzi osoba prawna, w ramach której ta instytucja obowiązana wykonuje swoje czynności zawodowe;
3) pomiędzy m.in. notariuszami, adwokatami, radcami prawnymi a ich klientami w zakresie informacji przekazywanych w celu zaprzestania przez klienta prowadzenia działalności sprzecznej z prawem lub powstrzymania klienta od podjęcia takiej działalności;
4) pomiędzy m.in. bankami krajowymi, instytucjami finansowymi mającymi siedzibę na terytorium RP, krajowymi instytucjami płatniczymi, firmami inwestycyjnymi, notariuszami, adwokatami, radcami prawnymi oraz pomiędzy tymi instytucjami obowiązanymi i ich odpowiednikami mającymi siedzibę w państwie członkowskim UE lub w państwie trzecim, które podlegają takim samym wymogom jak w AMLD lub równoważnym oraz stosują właściwe przepisy dotyczące tajemnicy zawodowej i ochrony danych osobowych, w przypadkach dotyczących tego samego klienta i tej samej transakcji.

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu 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 2015 Nr 141, str. 73 ze zm.).

W tym miejscu należy zwrócić uwagę, że żaden z wyżej przywołanych wyjątków nie odnosi się *explicite* do zrzeszenia banków spółdzielczych, tak jak ustawodawca czyni to w stosunku do grupy kapitałowej. Jednak z uwagi na podobieństwo funkcjonalne zrzeszenia banków spółdzielczych oraz grupy kapitałowej dalsze rozważania skupią się wyłącznie na wyjątkach określonych w art. 54 ust. 2 pkt 1 oraz art. 54 ust. 2 pkt 4 TerroryzmU.

1.6. Zrzeszenie jako *quasi* grupa kapitałowa?

Instytucje kredytowe i finansowe działające w ramach grupy mogą wymieniać się informacjami określonymi w art. 54 ust. 1 TerroryzmU. Zgodnie z art. 2 ust. 2 pkt 7 TerroryzmU grupa oznacza jednostkę dominującą wraz z jej jednostkami zależnymi oraz podmiotami, w których jednostki te mają udziały, oraz jednostkami powiązanymi ze sobą jednym ze związków, o których mowa w przepisach państw członkowskich UE wydanych na podstawie art. 22 SprawFinD[9]. Celem wyjaśnienia, decydującym aktem prawnym na gruncie unijnym w omawianym zakresie jest właśnie SprawFinD, do której w art. 3 pkt 15 (definicja grupy) bezpośrednio odwołuje się AMLD. Implementacja art. 22 SprawFinD do polskiego porządku prawnego nastąpiła w drodze nowelizacji RachunkU[10].

Zgodnie z art. 3 ust. 1 pkt 37 RachunkU, za jednostkę dominującą uważa się jednostkę będącą spółką handlową lub przedsiębiorstwem państwowym, sprawującą kontrolę nad jednostką zależną, w szczególności:

a) mającą bezpośrednio lub pośrednio większość ogólnej liczby głosów w organie stanowiącym jednostki zależnej, także na podstawie porozumień z innymi uprawnionymi do głosu, wykonującymi prawa głosu zgodnie z wolą jednostki dominującej, lub
b) będącą udziałowcem jednostki zależnej i uprawnioną do kierowania polityką finansową i operacyjną tej jednostki zależnej w sposób samodzielny lub przez wyznaczone przez siebie osoby lub jednostki na podstawie umowy zawartej z innymi uprawnionymi do głosu, mającymi na podstawie statutu lub umowy spółki, łącznie z jednostką dominującą, większość ogólnej liczby głosów w organie stanowiącym, lub
c) będącą udziałowcem jednostki zależnej i uprawnioną do powoływania i odwoływania większości członków organów zarządzających, nadzorujących lub administrujących tej jednostki zależnej, lub
d) będącą udziałowcem jednostki zależnej, której więcej niż połowę składu organów zarządzających, nadzorujących lub administrujących w poprzednim roku obroto-

[9] Dyrektywa Parlamentu Europejskiego i Rady 2013/34/UE z dnia 26 czerwca 2013 r. w sprawie rocznych sprawozdań finansowych, skonsolidowanych sprawozdań finansowych i powiązanych sprawozdań niektórych rodzajów jednostek, zmieniająca dyrektywę Parlamentu Europejskiego i Rady 2006/43/WE oraz uchylająca dyrektywy Rady 78/660/EWG i 83/349/EWG (Dz.Urz.UE.L 2013 Nr 182, str. 19 ze zm.).

[10] Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. 1994 Nr 121, poz. 591 ze zm.).

wym, w ciągu bieżącego roku obrotowego i do czasu sporządzenia sprawozdania finansowego za bieżący rok obrotowy stanowią osoby powołane do pełnienia tych funkcji w rezultacie wykonywania przez jednostkę dominującą prawa głosu w organach tej jednostki zależnej, chyba że inna jednostka lub osoba ma w stosunku do tej jednostki zależnej prawa, o których mowa w lit. a, c lub e, lub

e) będącą udziałowcem jednostki zależnej i uprawnioną do kierowania polityką finansową i operacyjną tej jednostki zależnej, na podstawie umowy zawartej z tą jednostką zależną albo statutu lub umowy tej jednostki zależnej.

Z kolei na podstawie art. 3 ust. 1 pkt 39 RachunkU za jednostkę zależną uznaje się jednostkę będącą spółką handlową lub podmiotem utworzonym i działającym zgodnie z przepisami obcego prawa handlowego, kontrolowaną przez jednostkę dominującą. Tak określona definicja jednostki dominującej jednoznacznie wskazuje, że dany podmiot może odgrywać rolę jednostki dominującej tylko wtedy, gdy ma bezpośrednio lub pośrednio większość ogólnej liczby głosów w organie stanowiącym jednostki zależnej, bądź jest jej udziałowcem (wspólnikiem) tudzież akcjonariuszem. Kierując się wykładnią językową, jednostką dominującą nie może być podmiot, który nie jest w żaden sposób zaangażowany kapitałowo w inny podmiot lub nie ma większości ogólnej liczby głosów w organie stanowiącym tego podmiotu (co w praktyce i tak sprowadza się do dysponowania odpowiednią liczbą udziałów lub akcji).

Ponadto definicja legalna jednostki zależnej (art. 3 ust. 1 pkt 39 RachunkU) określa, że taką jednostką może być wyłącznie spółka handlowa. Ustawodawca nie przewidział zatem, że potencjalnymi jednostkami zależnymi mogą być również spółdzielnie (w tym przypadku banki spółdzielcze), których podległość wobec podmiotu dominującego wynikałaby chociażby z okoliczności faktycznych[11]. Jednocześnie ustawodawca krajowy wyraźnie zawęził krąg potencjalnych jednostek zależnych w porównaniu do MSR[12]. Zgodnie bowiem z treścią Dodatku A do MSR jednostka zależna to po prostu podmiot, nad którym inna jednostka sprawuje kontrolę. Z kolei jednostka dominująca to jednostka, która sprawuje kontrolę nad jedną jednostką lub nad większą liczbą jednostek.

Rezultat wykładni językowej przywołanych przepisów RachunkU prowadzi zatem do jednoznacznego wniosku, że zrzeszenia banków spółdzielczych nie można utożsamiać z grupą w rozumieniu art. 2 ust. 2 pkt 7 TerroryzmU. Wprawdzie faktem jest, że to bank zrzeszający prowadzi sprawy i zarządza zrzeszeniem, a także reprezentuje banki spółdzielcze w stosunkach zewnętrznych, natomiast struktura wła-

[11] Por. art. 2 ust. 2 pkt 1 TerroryzmU, który nawiązuje do okoliczności faktycznych w zakresie sprawowania kontroli nad innym podmiotem. Zgodnie z przytoczoną regulacją, przez beneficjenta rzeczywistego rozumie się każdą osobę fizyczną sprawującą bezpośrednio lub pośrednio kontrolę nad klientem poprzez posiadane uprawnienia, które wynikają z okoliczności prawnych lub faktycznych, umożliwiające wywieranie decydującego wpływu na czynności lub działania podejmowane przez konkretny podmiot.

[12] Rozporządzenie Komisji (WE) nr 2023/1803 z 13.08.2023 r. przyjmujące określone międzynarodowe standardy rachunkowości zgodnie z rozporządzeniem (WE) nr 1606/2002 Parlamentu Europejskiego i Rady (Dz.Urz.UE.L 2023 Nr 237, str. 1 ze zm.).

snościowa oraz zaangażowania kapitałowego zrzeszania banków spółdzielczych cechuje się odmiennością w porównaniu do grup kapitałowych (jest odwrócona). Zrzeszenie banków spółdzielczych nie spełnia zatem kryteriów zawartych w, odczytywanym literalnie, art. 54 ust. 2 pkt 1 TerroryzmU (art. 3 ust. 1 pkt 37 i 39 RachunkU). W konsekwencji przekazywanie oraz gromadzenie informacji, o których mowa w art. 54 ust. 1 TerroryzmU, wewnątrz zrzeszenia banków spółdzielczych nie może odbywać się na podstawie wyjątku z art. 54 ust. 2 pkt 1 TerroryzmU.

W ocenie autorów rezultat wykładni językowej nie pozwala realizować celu zakładanego przez prawodawcę i nie służy dobrze funkcjonującemu mechanizmowi przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Właściwe przepisy RachunkU determinujące pozycję jednostek dominujących oraz zależnych swoje źródło mają w regulacjach SprawFinD. Dla ustawodawcy krajowego, ale również i dla podmiotów, które muszą podporządkować się określonym obowiązkom, regulacje unijne wyznaczają pewien wzorzec interpretacyjny, który może kreować następczo sposób postępowania jednostki na gruncie prawa krajowego. Jednak art. 22 SprawFinD, który wyznacza zakres definicji grupy na gruncie TerroryzmU (jak również na gruncie AMLD), odnosząc się do jednostek dominujących oraz zależnych, również utożsamia stosunek istniejący pomiędzy tymi podmiotami z tradycyjnym zaangażowaniem kapitałowym tudzież własnościowym. Odzwierciedleniem powyższego jest treść przywołanego art. 3 ust. 1 pkt 37 RachunkU.

Mając na uwadze powyższe, zarówno ustawodawca unijny, a w ślad za nim prawodawca krajowy, nie utożsamiają banku zrzeszającego z jednostką dominującą w stosunku do podmiotów należących do zrzeszenia. Całkowicie została pominięta również sytuacja spółdzielni (*ergo* banków spółdzielczych), gdyż przytoczone przepisy, w zakresie ustalenia statutu jednostki dominującej, traktują wyłącznie o posiadaniu statusu wspólnika lub akcjonariusza. Oznacza to, że kierowanie się wykładnią prounijną w omawianym zakresie z potencjalną korzyścią dla sytuacji banków należących do zrzeszeń banków spółdzielczych nie jest możliwe.

Z innej jednak strony, odnosząc się do funkcji jaką bank zrzeszający pełni w zrzeszeniu banków spółdzielczych, a także mając na uwadze przyznane mu uprawnienia, stosując wykładnię funkcjonalną, zrzeszenie banków spółdzielczych powinniśmy móc zakwalifikować do kategorii *quasi* grupy kapitałowej. Nie bez znaczenia dla analizowanego zagadnienia pozostaje bowiem fakt, że zgodnie z art. 19 ust. 2 pkt 7 BankSpółU bank zrzeszający reprezentuje, a także jest przedstawicielem zrzeszonych banków spółdzielczych w stosunkach zewnętrznych w sprawach wynikających z umowy zrzeszenia (Spyra 2011). Wobec powyższego bank zrzeszający działa w charakterze przedstawiciela ustawowego banków spółdzielczych, które to uprawnienie wynika *explicite* z ustawy. Może to sugerować, że kierując się jednocześnie względami natury praktycznej, prawidłowe byłoby przyjęcie, że bank zrzeszający wspólnie z bankami spółdzielczymi są uprawnione do wymiany informacji, o których mowa w art. 54 ust. 1 TerroryzmU. Wniosek taki ma jednak jedną, podstawową wadę, a mianowicie – przeczy jednoznacznemu rezultatowi wykładni językowej.

W doktrynie wskazuje się także na fakt, że stosunki między bankami zrzeszonymi odpowiadają stosunkom prawnym i faktycznym panującym w koncernach, zarówno w aspekcie horyzontalnym, jak i wertykalnym (Szczęśniak 2022). Pojęcie koncernu nie zostało jednak zdefiniowane w polskim porządku prawnym. Strukturę koncernową definiuje się w piśmiennictwie jako zgrupowanie prawnie samodzielnych przedsiębiorców powiązanych faktycznie lub formalnie. Koncern jest bowiem formą współdziałania przedsiębiorców, którzy zachowują swoją odrębność prawną (Rieder i Haumer 2019). Oznacza to, że uczestnicy koncernu są samodzielnymi podmiotami prawa (Radwański 2009), są zatem odrębnymi od koncernu podmiotami stosunków prawnych (Frąckowiak 2005).

W nauce wskazuje się ponadto, że przedsiębiorcy tworzący strukturę koncernową powinni pozostawiać pod wspólnym kierownictwem (Stecki 2001). Stosunki prawne i faktyczne między przedsiębiorcami opierają się na podporządkowaniu jednemu podmiotowi kierowniczemu (Włodyka 2003). W stosunkach uczestników koncernu jest tym samym widoczny element podporządkowania (Lutter, Scheffler i Schneider 1998). Podporządkowanie przedsiębiorców względem określonego podmiotu kierowniczego odróżnia koncern od innych form koncentracji gospodarczej.

1.7. Ten sam klient, ta sama transakcja

Drugi z wyjątków wyrażony w art. 54 ust. 2 pkt 4 TerroryzmU odnosi się do sytuacji gromadzenia oraz wymiany informacji, o których mowa w art. 54 ust. 1 TerroryzmU, natomiast wyłącznie w przypadkach dotyczących tego samego klienta i tej samej transakcji. Posiłkując się tym wyjątkiem, należy zatem zachować tożsamość po stronie podmiotowej oraz przedmiotowej transakcji. Przy tej konstrukcji przepisu możliwe jest ujawnienie informacji jedynie przy spełnieniu wszystkich przesłanek w sposób łączny, a zatem np. w odniesieniu do transakcji przelewu pomiędzy rachunkami tej samej osoby. Jeśli natomiast podejrzenie dotyczyłoby przekazu z jednego do drugiego banku, ale np. z rachunku osoby fizycznej na rachunek osoby prawnej, w której ta osoba fizyczna jest beneficjentem rzeczywistym, taka sytuacja nie korzysta już ze zwolnienia wskazanego w tym przepisie (Obczyński 2023).

1.8. Tajemnica bankowa w kontekście przekazywania informacji istotnych z perspektywy AML/CFT

Wyjaśnienia wymagają także regulacje PrBank dotyczące przekazywania informacji objętych tajemnicą bankową, celem wykonywania obowiązków w zakresie określonym w przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Zgodnie z art. 104 PrBank, bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje dotyczące czynności

bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje.

Tajemnicę bankową stanowią zarówno informacje dotyczące czynności bankowej jako takiej, jak i informacje dotyczące osoby lub osób dokonujących z bankiem tej czynności bankowej (Smykla i Dietrich 2005). W stosunku do banków będą to czynności wymienione w art. 5 ust. 1 i 2 PrBank, w przypadku innych podmiotów wykonujących działalność bankową – wyłącznie czynności bankowe wyliczone w art. 5 ust. 1 PrBank (Smykla 2000). Katalog czynności bankowych z PrBank pokrywa się z katalogiem czynności bankowych, które mogą wykonywać banki spółdzielcze (art. 6 ust. 1 BankSpółU). Należy wobec tego uznać, że proces polegający na gromadzeniu oraz wymianie informacji dotyczących konkretnych klientów, dla których podmioty należące do zrzeszenia banków spółdzielczych przechowują środki pieniężne oraz przeprowadzają na ich zlecenie rozliczenia pieniężne, podlega tajemnicy bankowej, o której mowa w art. 104 PrBank.

Trzeba jednak pamiętać, że celem gromadzenia oraz wymiany informacji jest ułatwienie zaangażowanym podmiotom identyfikacji osób o potencjalnie wyższym ryzyku prania pieniędzy i finansowania terroryzmu podczas bieżącego monitorowania transakcji. Jest to kluczowe z uwagi na treść art. 106d ust. 1 pkt 3 PrBank, który stanowi, że banki oraz inne instytucje finansowe (tamże wymienione) mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową, w przypadkach wykonywania obowiązków w zakresie określonym w przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Jest to o tyle istotne, gdyż analizowany art. 54 ust. 1 TerroryzmU istotnie zawęża możliwość stosowania art. 106d PrBank, ponieważ wyklucza z wymiany fakt przekazania zawiadomienia do GIIF oraz informacje o planowaniu wszczęcia oraz o prowadzeniu analizy dotyczącej prania pieniędzy lub finansowania terroryzmu, co byłoby najbardziej interesujące oraz pożądane dla zaangażowanych podmiotów.

Art. 106d ust. 1 pkt 3 PrBank nie wprowadza dodatkowych ograniczeń (jak np. przywołany art. 104 ust. 2) w zakresie wymiany pomiędzy bankami informacji dotyczących wykonywania obowiązków wynikających z regulacji służących przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Wprawdzie regulacje TerroryzmU oraz PrBank są niezależne od siebie, natomiast redakcja art. 106d ust. 1 pkt 3 TerroryzmU nakazuje uznać, że instytucji finansowe mogą korzystać ze zwolnienia z tajemnicy bankowej na potrzeby wykonywania obowiązków dotyczących przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu wyłącznie w takim zakresie w jakim zostało to określone w TerroryzmU.

Wydaje się zatem, że o ile na gruncie PrBank (biorąc pod uwagę treść art. 106d ust. 1 pkt 3 PrBank), celem spełnienia obowiązków z zakresu przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu, instytucje finansowe mogą w sposób szeroki i pełniejszy przetwarzać oraz wzajemnie udostępniać informacje (w tym informacje objęte tajemnicą bankową), o tyle na gruncie TerroryzmU możliwość ta jest znacznie ograniczona.

Informacje, które miałyby być przedmiotem wymiany w zrzeszeniu banków spółdzielczych mają charakter czynności, o których mowa w art. 54 ust. 1 pkt 2 TerroryzmU, a zatem są objęte zakazem ich ujawniania osobom nieuprawnionym. Sama wykładnia językowa przepisu art. 106d ust. 1 pkt 3 PrBank wskazuje, że instytucje finansowe mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową, w przypadkach wykonywania obowiązków w zakresie określonym w przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Zakres przekazywania informacji, o którym mowa w zdaniu poprzednim, został wyznaczony chociażby w szerzej analizowanym powyżej art. 54 TerroryzmU.

Pomimo ogólnego uprawnienia instytucji finansowych do ujawniania informacji stanowiących tajemnicę bankową w zakresie określonym w przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, art. 54 ust. 1 TerroryzmU może stanowić *lex specialis* wobec regulacji art. 106d ust. 1 pkt 3 PrBank, wyraźnie ograniczając możliwość przekazania informacji pomiędzy instytucjami finansowymi.

2. Potrzeba zmian

Sytuacja zrzeszenia banków spółdzielczych na gruncie TerroryzmU w zakresie możliwości wymiany informacji jest skomplikowana oraz niejednoznaczna. Ustawodawca krajowy, podczas tworzenia odpowiednich regulacji z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, całkowicie pominął strukturę jakim jest zrzeszenie banków spółdzielczych. Podobnie ustawodawca unijny, w trakcie projektowania AMLD (stanowiącej źródło przepisów nakładających na określone podmioty obowiązki związane z AML/CFT) oraz SprawFinD, nie pochylił się w sposób szczególny nad sytuacją zrzeszeń banków spółdzielczych, które stanowią przecież istotną część sektora finansowego nie tylko w Polsce, ale również w pozostałych krajach europejskich (Alińska 2017)[13], tworząc typowo komercyjne specjalistyczne instytucje finansowe, jak instytucje leasingowe, inwestycyjne czy faktoringowe (Gniewek 2005).

Należy jednak stwierdzić, odnosząc się jedynie do Dodatku A do MSR, że ustawodawca unijny pozostawił szersze pole do wykładni przepisów aniżeli ustawodawca polski, co akurat w tym przypadku należy ocenić pozytywnie. Jednakże podstawę działań banków spółdzielczych oraz kierunki interpretacyjne w analizowanym zakresie wyznaczają przepisy RachunkU, które implementują do naszego porządku prawnego regulacje unijne. Niewątpliwie efektem takiej niekonsekwencji pozostają

[13] W Polsce przykładami zrzeszeń banków spółdzielczych są: Spółdzielcza Grupa Bankowa (SGB-Bank S.A. jako bank zrzeszający) oraz Grupa Banku Polskiej Spółdzielczości S.A. (Bank Polskiej Spółdzielczości S.A. jako bank zrzeszający). Zrzeszenia banków spółdzielczych w Europie tworzą m.in. DZ Bank (Niemcy), Crédit Agricole (Francja), Rabobank (Holandia).

trudności w wykładni oraz praktyczne problemy w sprawnym funkcjonowaniu instytucji obowiązanych jakimi są banki spółdzielcze.

Aby wyeliminować opisaną wątpliwość prawną należałoby rozważyć zmianę definicji legalnej grupy na gruncie TerroryzmU, która wprost przewidywałaby, że na potrzeby przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, za grupę uznaje się również zrzeszenie banków spółdzielczych. Inną możliwością byłoby poszerzenie katalogu wyłączeń z art. 54 ust. 2 TerroryzmU dodając, że obowiązek zachowania w tajemnicy informacji nie dotyczy przekazywania informacji pomiędzy bankami należącymi do zrzeszenia banków spółdzielczych[14].

Alternatywnym rozwiązaniem pozostawałaby zamiana definicji jednostki dominującej oraz jednostki zależnej na gruncie RachunkU, nie ograniczając ich wyłącznie do podmiotów zaangażowanych kapitałowo w inny podmiot (definicja jednostki dominującej), bądź wyłącznie do podmiotów będących spółkami handlowymi (definicja jednostki zależnej). Pewnym odniesieniem w tym zakresie powinna być ogólna definicja jednostki dominującej oraz zależnej z Dodatku A do MSR.

Bibliografia

Alińska A. (2017), *Specyfika działalności i wyniki finansowe sektora banków spółdzielczych w Europie*, [w:] *Współczesna bankowość spółdzielcza*, red. A. Szelągowska, Warszawa.

Bączyk M. (2020), *Bankowość spółdzielcza w systemie prawa spółdzielczego*, [w:] *System Prawa Prywatnego*, t. 21, *Prawo spółdzielcze*, red. K. Pietrzykowski, Warszawa.

Frąckowiak J. (2005), *Jednostka organizacyjna jako substrat osoby prawnej i ustawowej*, [w:] *Rozprawy prawnicze. Księga pamiątkowa Profesora Maksymiliana Pazdana*, red. L. Ogiełło, W. Popiołek, M. Szpunar, Kraków.

Gniewek J. (2005), *Funkcjonowanie spółdzielczego sektora bankowego w Polsce po akcesji Polski do Unii Europejskiej*, [w:] *Agrobiznes – Zmiany w agrobiznesie po przystąpieniu Polski do Unii Europejskiej*, t. 1, red. S. Urban, Wydawnictwo Akademii Ekonomicznej im. O. Langego, Wrocław.

Lutter M., Scheffler E., Schneider U.H. (1998), *Der Konzern als finanzwirtschaftliche Einheit*, [w:] *Handbuch der Konzernfinanzierung*, Köln.

Obczyński R. (2023), [w:] *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. M. Nowakowski, Warszawa, art. 54.

Radwański Z. (2009), *Prawo cywilne – część ogólna*, Warszawa.

Rieder B., Huemer D. (2019), *Gesellschaftsrecht*, Wiedeń.

[14] Punkt odniesienia w zakresie możliwości wymiany potrzebnych informacji na gruncie TerroryzmU pomiędzy instytucjami obowiązanymi może stanowić również niemiecki odpowiednik TerroryzmU, tj. Geldwäschegesetz – GwG, który w § 47 ust. 5 stanowi, że podmioty zobowiązane, zgodnie z § 2 ust. 1 pkt 1–9 mogą przekazywać sobie wzajemnie informacje o określonych faktach zawierających nieprawidłowości lub nietypowe cechy wskazujące na pranie pieniędzy, jeśli założą, że inne strony zobowiązane mogą potrzebować tych informacji.

Smykla B. (2000), *Tajemnica bankowa – wybrane zagadnienia*, „Radca Prawny", Nr 3.

Smykla B., Dietrich M. (2005), *Problemy nowelizacji Prawa bankowego*, MoP, Nr 7.

Spyra M. (2011), *Funkcjonowanie banków spółdzielczych, ich zrzeszanie się i banki zrzeszające. Komentarz*, Warszawa.

Stecki L. (2001), *Koncern*, Toruń.

Szczęśniak P. (2019), *Banki*, [w:] *Prawo finansowe. Wybrane zagadnienia*, red. A. Hanusz, Warszawa.

Szczęśniak P. (2022), *Zgrupowania solidarnościowe banków spółdzielczych. Konstrukcja normatywna*, Warszawa.

Włodyka S. (2003), *Prawo koncernowe*, Kraków.

Zalcewicz A. (2009), *Bank spółdzielczy. Aspekty prawne tworzenia i funkcjonowania*, Warszawa.

DOI: 10.26354/bb.5.1.94.2024

Jan Szczygieł*
ORCID: 0000-0001-8273-614X
Jan.Szczygiel@bfg.pl

Dematerializacja listów zastawnych w kontekście zmian regulacyjnych

Streszczenie

Artykuł prezentuje zagadnienia związane z funkcjonowaniem na rynkach finansowych listów zastawnych w formie zdematerializowanej. Omówiono w nim jednak nie tylko formy funkcjonowania listów zastawnych jako papierów wartościowych, lecz również rolę, jaką odgrywa dematerializacja listów zastawnych w funkcjonowaniu rynku papierów wartościowych. Zachodzące zmiany technologiczne, zwłaszcza w kontekście rozwoju technologii łańcucha bloków (ang. *blockchain*), skłaniają do podjęcia dyskusji na tle przyszłości formy funkcjonowania listów zastawnych w obrocie, a zwłaszcza możliwość ich tokenizacji[1]. Poruszane w artykule zagadnienia nie doczekały się do tej pory całościowego opracowania w piśmiennictwie. Podstawowym celem badawczym było wykazanie, po pierwsze, że dematerializacja listów zastawnych pozytywnie wpływa na elastyczność emisji tych papierów wartościowych. Po drugie, że dematerializacja jest bezpiecznym rozwiązaniem inkorporowania papierów wartościowych, jednak niepozbawionym całkowicie ryzyk.

W artykule posłużono się metodą dogmatyczno-prawną (Pieter 1975, s. 25). Jej przedmiotem była analiza przepisów prawa oraz ich wykładnia. Metoda ta pozwoliła ustalić obowiązujące przepisy w omawianym zakresie i dostrzec zachodzące zmiany regulacyjne w kontekście formy funkcjonowania listów zastawnych jako papierów wartościowych.

Słowa kluczowe: listy zastawne, papiery wartościowe, banki hipoteczne, dematerializacja listów zastawnych, technologia łańcucha bloków

Kody JEL: K10, G21

* Jan Szczygieł – dr nauk prawnych, radca prawny, Bankowy Fundusz Gwarancyjny.

1 Pod pojęciem tokenizacji należy rozumieć: „cyfrowe odzwierciedlenie instrumentów finansowych w rozproszonych rejestrach lub emisję tradycyjnych klas aktywów w formie tokenów w celu umożliwienia ich emisji, przechowywania i przenoszenia w rozproszonym rejestrze", zob. Serzysko 2023.

Dematerialization of covered bonds in the context of regulatory changes

Abstract

The article presents issues related to the functioning of dematerialized covered bonds on financial markets. The article discusses not only the forms of functioning of covered bonds as securities, but also the role played by the dematerialization of covered bonds in the functioning of the securities market. The ongoing technological changes, especially in the context of the development of blockchain technology, prompt discussion on the future form of functioning of covered bonds in trade, and especially the possibility of their tokenization. The issues discussed in the article have not yet been comprehensively treated in the literature. The basic research goal was to demonstrate that the dematerialization of covered bonds has a positive impact on the flexibility of the issuance of these securities. Secondly, dematerialization is a safe solution for the incorporation of securities, but not completely without risks. Thirdly, and finally, although it seems technologically possible to issue covered bonds as part of tokenization, this change requires the introduction of systemic regulatory changes.

The article uses the dogmatic-legal method. Its subject was the analysis of legal provisions and their interpretation. This method made it possible to determine the applicable regulations in the discussed area and to notice the ongoing regulatory changes in the context of the form of functioning of covered bonds as securities.

Keywords: covered bonds, securities, mortgage banks, dematerialization of covered bonds, blockchain

JEL Codes: K10, G21

Wstęp

Listy zastawne są papierami wartościowymi, stanowiącymi bezpieczny i stabilny instrument finansowy (Mekiński 2001, s. 2). Korzystnie oddziałują na stabilność systemu finansowego (Dżuryk 2018, s. 73). Jakkolwiek aktualnie materię funkcjonowania w obrocie listów zastawnych reguluje ustawa z 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych (Dz.U. 2023 poz. 110 ze zm.; dalej: u.l.z.b.h.), to jednak listy zastawne stanowią papiery wartościowe o wielowiekowej tradycji[2]. Instytucja listów zastawnych czerpie z doświadczeń starożytnej hipoteki greckiej, włoskich listów dłużnych, czy niderlandzkich listów kolonialnych (Kaszubski i Olszak 2000, s. 15). Jednakże zasadnicze dla rozwoju bankowości hipotecznej i instytucji listów zastawnych miało powołanie z dniem 5 lipca 1770 r. Śląskiego Towarzystwa Kredytowego Ziemskiego (niem. *Schlesische Landschaften*) (Sattler 2019, s. 25 i n.). Kolejne stulecia przynosiły dalszy rozwój bankowości hipotecznej, aż do wybuchu II wojny światowej (Bellinger 1994, s. 4). Ostatnie dekady przyczyniły się do renesansu instytucji listu zastawnego i jego szczególnego rozwoju.

[2] Szerzej na temat historii listu zastawnego zob. Kanigowski 2019.

Celem opracowania jest ocena zmian regulacyjnych odnoszących się do formy emisji listów zastawnych wprowadzających zasadę dematerializacji listów zastawnych. Artykuł zmierza do zaprezentowania zagadnień związanych z funkcjonowaniem na rynkach finansowych listów zastawnych w kontekście form, w jakich papiery te mogą występować w obrocie. Problematyka dematerializacji listów zastawnych ma charakter wieloaspektowy i z pewnością wykraczający poza ramy niniejszego opracowania. Autor omawia nie tylko formy funkcjonowania listów zastawnych jako papierów wartościowych, lecz skupia się również na wskazaniu roli dematerializacji listów zastawnych w funkcjonowaniu rynku papierów wartościowych. Funkcjonowanie papierów wartościowych w zmieniających się realiach, wraz z rozwojem technik komputerowych, wymaga dostosowania do zmieniających się warunków obrotu na rynku kapitałowym. Zachodzące zmiany technologiczne, zwłaszcza w kontekście rozwoju technologii łańcucha bloków (ang. *blockchain*)[3], skłaniają do podjęcia dyskusji na tle zmian regulacyjnych odnoszących się do formy funkcjonowania listów zastawnych w obrocie prawnym, a zwłaszcza możliwości ich tokenizacji[4]. Omawiane zagadnienie dematerializacji listów zastawnych nie doczekało się do tej pory całościowego opracowania w piśmiennictwie. Podstawowym celem badawczym jest wykazanie, że dematerializacja listów zastawnych pozytywnie wpływa na elastyczność emisji tych papierów wartościowych i zwiększa bezpieczeństwo obrotu niwelując ryzyka jakie niesie za sobą tradycyjna, dokumentowa forma papieru wartościowego. Ponadto artykuł zmierza do wykazania, że dematerializacja stanowi bezpieczne rozwiązanie inkorporowania papierów wartościowych, jednak niepozbawione całkowicie ryzyk.

Główną rolę podczas weryfikacji powyższych hipotez odgrywała metoda dogmatyczno-prawna. W artykule w pierwszej kolejności analizie poddano obowiązujące przepisy prawa. Dążąc do ustalenia wynikających z tych przepisów norm prawnych, poddano je odpowiedniej wykładni. Metoda dogmatyczno-prawna pozwoliła dostrzec zachodzące zmiany regulacyjne w kontekście formy funkcjonowania listów zastawnych jako papierów wartościowych. Wspomagająco, sięgając do dotychczasowych opracowań doktryny, posłużono się również metodą teoretycznoprawną.

1. Formy listów zastawnych

Kryterium podziału papierów wartościowych ze względu na nośnik praw wyrażonych w papierze wartościowym stanowi jedno z kryteriów doktrynalnej klasyfikacji papierów wartościowych (Romanowski 2016, s. 78)[5]. W systemach prawnych

[3] Pod pojęciem technologii łańcucha bloków (ang. *blockchain*) rozumie się rejestr pod postacią rozproszonej bazy danych (Distributed Ledger Technology) obejmujący powiązane ze sobą bloki informacji, w ten sposób, że każdy z kolejnych bloków informacji zawiera oznaczenie czasu jego stworzenia (*timestamp*) oraz link do poprzedniego bloku, będący zaszyfrowanym „streszczeniem" (*hash*) jego zawartości, tworząc jako całość nierozerwalny łańcuch. Zob. Piech 2016.

[4] Pod pojęciem tokenizacji należy rozumieć: „cyfrowe odzwierciedlenie instrumentów finansowych w rozproszonych rejestrach lub emisję tradycyjnych klas aktywów w formie tokenów w celu umożliwienia ich emisji, przechowywania i przenoszenia w rozproszonym rejestrze", zob. Serzysko 2023.

[5] Autor ten do pozostałych kryteriów klasyfikacji doktrynalnej papierów wartościowych zalicza podział ze względu na: przedmiot praw inkorporowanych w dokumencie, sposób określenia w doku-

wyróżnia się dwie koncepcje formy papierów wartościowych: materialną oraz zdematerializowaną (Chłopecki 1995, s. 13 i n.; Świderska-Iwicka 1995, s. 26 i n.)[6].

Materialna forma papierów wartościowych oznacza powiązanie prawa materialnego z fizycznie istniejącym dokumentem będącym formą trwałego nośnika informacji[7]. Papiery wartościowe funkcjonujące w tej formie pełniły podstawową funkcję legitymacyjną, w której zawierało się zarówno uprawnienie dłużnika do zwolnienia się z wynikającego z papieru wartościowego świadczenia[8], jak i posiadacza papieru wartościowego, legitymowanego do żądania spełnienia świadczeń wyłącznie przez okazanie dokumentu papieru wartościowego (Chłopecki 2006, s. 878).

Z kolei pod pojęciem dematerializacji listu zastawnego należy rozumieć brak substratu materialnego tego papieru wartościowego[9], a jego funkcjonowanie uwidocznione jest w formie elektronicznego wpisu we właściwym rejestrze (Romanowski 2016, s. 114). Dematerializacja stanowi odstępstwo od tradycyjnej formy papieru wartościowego jaką jest forma dokumentu. Dematerializacja papierów wartościowych i postępujące odejście od materialnej formy papierów wartościowych wykreowały zasadę dematerializacji obrotu tymi papierami (Chłopecki 2006, s. 874).

2. Materialna forma listu zastawnego

Jakkolwiek ustawa o listach zastawnych i bankach hipotecznych statuuje generalną zasadę dematerializacji listów zastawnych, to jednak art. 5a ust. 2 u.l.z.b.h. stanowi odstępstwo od tej zasady, dopuszczając emitowanie listów zastawnych, w warunkach określonych w tym przepisie, w tradycyjnej formie dokumentu. W brzmieniu pierwotnym, nadanym ustawą z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku[10], art. 5a ust. 2 dopuszczał formę dokumentu dla listu zastawnego o jednostkowej wartości nominalnej przekraczającej kwotę stanowiącą równowartość 100 000 euro, ustaloną przy zastosowaniu średniego kursu euro ogłoszonego przez Narodowy Bank Polski w dniu podjęcia przez emitenta decyzji o emisji.

mencie osoby uprawnionej, sposób przenoszenia praw inkorporowanych w dokumencie, zależność między powstaniem prawa inkorporowanego w dokumencie a powstaniem dokumentu, zdolność zamiany na inny typ papieru wartościowego, sposób uzyskania statusu papieru wartościowego, funkcję spełnianą w obrocie.

6 Tam też o kształtowaniu się poglądów odnośnie do zdematerializowanej formy papierów wartościowych.

7 W zakresie pojęcia trwałego nośnika zob. Szczygieł 2017, s. 20–23.

8 Por. art. 921 (7) ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2023 poz. 1610 z późn. zm.), zgodnie z którym spełnienie świadczenia do rąk posiadacza legitymowanego treścią papieru wartościowego zwalnia dłużnika, chyba że działał on w złej wierze.

9 Por. Michalski 1999, s. 134; 2006, s. 506. Bliżej o koncepcji papierów wartościowych w kontekście dematerializacji ich formy zob. Jastrzębski 2009.

10 Ustawa z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku (Dz.U. poz. 2243 z późn. zm.).

Aktualne brzmienie ust. 2 zostało nadane z dniem 8 lipca 2022 r. mocą art. 1 pkt 4 ustawy z dnia 7 kwietnia 2022 r. o zmianie ustawy o listach zastawnych i bankach hipotecznych oraz niektórych innych ustaw (Dz.U. 2022, poz. 872). Jak podkreślono w uzasadnieniu projektu ustawy nowelizującej art. 5a ust. 2 u.l.z.b.h., zmiana ta pozwoli na emisję listów zastawnych w formie dokumentu w przypadku listów zastawnych o jednostkowej wartości nominalnej równej kwocie stanowiącej równowartość 100 000 euro lub przekraczającej tę kwotę. Przepis ten w obecnym brzmieniu umożliwia emisję listu zastawnego w formie dokumentu, o ile jego wartość nominalna przekracza równowartość 100 000 euro[11]. Dalej zauważono, że listy zastawne o jednostkowej wartości nominalnej nie niższej niż równowartość 100 000 euro stanowią nominał występujący często w praktyce obrotu zagranicznego. Dlatego też, w ocenie ustawodawcy, dokonana zmiana brzmienia art. 5a ust. 2 ma szczególne znaczenie w odniesieniu do listów zastawnych oferowanych na międzynarodowych rynkach i ich rejestrowania w zagranicznym systemie rejestracji, o którym mowa w art. 5 ust. 1a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi[12].

List zastawny, o którym mowa w art. 5a ust. 2, podlega zarejestrowaniu w depozycie papierów wartościowych prowadzonym zgodnie z przepisami ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi. Artykuł 5a ust. 4 określa szczegółowe zasady rejestracji listu zastawnego w przypadku, o którym mowa w art. 5 ust. 1a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, a więc w sytuacji, w której emitent zamierza zarejestrować papiery wartościowe w innym systemie rejestracji – w terminie 6 miesięcy od dnia emisji. Dematerializacja takich listów zastawnych, zgodnie z art. 49 ust. 1 rozporządzenia 909/2014[13], następuje z chwilą zarejestrowania w tym systemie, jeżeli podmiot prowadzący ten system spełnił warunki, o których mowa w art. 23 tego rozporządzenia. Należy bowiem podkreślić, że w myśl art. 49 ust. 1 rozporządzenia 909/2014, statuującego swobodę emisji w ramach Centralnego depozytu papierów wartościowych (dalej: CDPW) posiadającego zezwolenie w Unii Europejskiej, emitent ma prawo poczynić kroki w celu zarejestrowania swoich papierów wartościowych dopuszczonych do obrotu na rynkach regulowanych lub wielostronnej platformie obrotu lub będących przedmiotem obrotu w systemach obrotu w dowolnym CDPW z siedzibą w dowolnym państwie członkowskim, z zastrzeżeniem spełnienia przez dany CDPW warunków, o których mowa w art. 23 tego rozporządzenia. Bez uszczerbku dla prawa emitenta, o którym mowa w akapicie pierwszym, przepisy prawa spółek i inne podobne przepisy państwa członkowskiego, na mocy których dane papiery wartościowe powstały, nadal mają zastosowanie.

[11] Uzasadnienie rządowego projektu ustawy o zmianie ustawy o listach zastawnych i bankach hipotecznych oraz niektórych innych ustaw, Sejm IX kadencji, druk Sejm. nr 2019, s. 9.

[12] *Ibidem*.

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz.U.UE L z 2014 r. Nr 257, str. 1 z późn. zm.).

3. Dematerializacja listów zastawnych

Sednem dematerializacji papierów wartościowych jest zastąpienie materialnego dokumentu stanowiącego substrat praw wartościowych na niematerialny, niemający fizycznej postaci dokumentu, zespół danych komputerowych, co ma z jednej strony usprawnić obrót papierami wartościowymi, z drugiej strony natomiast stanowić zwiększenie buforu bezpieczeństwa obrotu prawami z papierów wartościowych (Romanowski 2016, s. 114). Trafnie w tym aspekcie wskazuje się, że dematerializacja papierów wartościowych, w tym listów zastawnych, niweluje ryzyka jakie wiążą się z inkorporowaniem papierów wartościowych w formie dokumentu, a mianowicie utraty, zniszczenia lub uszkodzenia dokumentu.

Mając na względzie postępujące zmiany w obrocie papierami wartościowymi, z dniem 1 lipca 2019 r., w drodze zmian legislacyjnych dokonanych ustawą z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku[14], wprowadzono do ustawy o listach zastawnych i bankach hipotecznych art. 5a. Przepis ten statuuje obligatoryjną zasadę dematerializacji listów zastawnych wraz z obowiązkową rejestracją w depozycie papierów wartościowych prowadzonym przez Krajowy Depozyt Papierów Wartościowych (dalej: KDPW). KDPW wykonuje zadania określone w ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U. 2024 poz. 722; dalej: u.o.i.f.), to jest:

- prowadzi depozyt papierów wartościowych;
- wykonuje czynności w zakresie prowadzenia systemu rejestracji instrumentów finansowych niebędących papierami wartościowymi ani instrumentami pochodnymi, które zostały dopuszczone do obrotu na rynku regulowanym lub wprowadzone do Alternatywnego Systemu Obrotu;
- nadzoruje zgodność wielkości emisji z liczbą papierów wartościowych, zarejestrowanych w depozycie papierów wartościowych, znajdujących się w obrocie;
- obsługuje realizację zobowiązań emitentów wobec uprawnionych z papierów wartościowych zarejestrowanych w depozycie papierów wartościowych;
- wykonuje czynności związanych z wycofywaniem papierów wartościowych z depozytu papierów wartościowych;
- dokonuje rozrachunku w instrumentach finansowych i środkach pieniężnych w związku z transakcjami zawieranymi na rynku regulowanym oraz transakcjami zawieranymi w ASO w zakresie instrumentów finansowych zarejestrowanych w Krajowym Depozycie;
- zapewnia prawidłowe funkcjonowanie obowiązkowego systemu rekompensat.

W zamyśle projektodawcy wprowadzona zmiana miała sprzyjać zwiększeniu transparentności emisji dłużnych papierów wartościowych, a co za tym idzie bezpie-

[14] Zob. art. 4 pkt 1 ustawy z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku (Dz.U. 2018 poz. 2243).

czeństwu i elastyczności dla inwestorów[15]. Cel ten, w mojej ocenie, należy uznać za spełniony. Przede wszystkim, w aspekcie bezpieczeństwa, dematerializacja papierów wartościowych minimalizuje ryzyka na jakie potencjalnie narażone są papiery wartościowe w formie dokumentu jako nośnika informacji (m.in. kradzież czy uszkodzenie). Podkreślenia wymaga, że w uzasadnieniu wprowadzonej zmiany wyrażono przekonanie, że: „system rejestracji prowadzony przez KDPW jest systemem najbezpieczniejszym (ewidencja jest nadzorowana przez KNF oraz przez KDPW), a rejestracja w tym systemie wszystkich niepublicznych papierów dłużnych doprowadzi do tego, że rejestrować je będą jedynie podmioty najlepiej przygotowane do tego zadania, czyli domy maklerskie i banki posiadające zezwolenie na prowadzenie rachunków papierów wartościowych i będące uczestnikami KDPW, a nie – jak dotychczas – także podmioty, które nie są uprawnione do prowadzenia rachunków papierów wartościowych. Ponadto inwestor będzie miał możliwość przenoszenia aktywów do innych podmiotów”[16].

4. Domniemanie zasady dematerializacji

Normatywną podstawę do funkcjonowania w polskim systemie prawnym zasady dematerializacji papierów wartościowych wyraża art. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi. Ustawa ta, w drodze odesłania zawartego w art. 8 ust. 1 pkt 2 u.l.z.b.h., znajduje odpowiednie zastosowanie w zakresie nieuregulowanym ustawą o listach zastawnych i bankach hipotecznych do zasad emisji, obrotu i wykupu hipotecznych listów zastawnych. Artykuł 7 ust. 1 u.o.i.f. określa moment powstania zdematerializowanych papierów wartościowych wskazując, że prawa ze zdematerializowanych papierów wartościowych powstają z chwilą zapisania ich po raz pierwszy na rachunku papierów wartościowych i przysługują osobie będącej posiadaczem tego rachunku, z zastrzeżeniem art. 7a ust. 7a u.o.i.f. Wykładnia tego przepisu prowadzi do wniosku, że przesłanką powstania zdematerializowanych papierów wartościowych jest pierwszy wpis tych papierów wartościowych na rachunku (Sójka i Godlewski 2022).

Pomimo wprowadzenia domniemania zasady dematerializacji sprowadzającej się do prostego zanegowania formy dokumentu listu zastawnego, art. 5a u.l.z.b.h. nie określa precyzyjnie jego formy zdematerializowanej, na przykład formy elektronicznego pliku w jakim jest on zapisany. W piśmiennictwie trafnie przyjmuje się jednak, że dematerializacja papieru wartościowego, a więc i listu zastawnego, nie oznacza całkowitej likwidacji nośnika materialnego, a jedynie prowadzi do zmiany postaci nośnika treści papieru wartościowego z papierowej do elektromagnetycznego wpisu komputerowego (Pietrasik i Laskowski 2001, s. 219). Wprowadzenie do

[15] Zob. Uzasadnienie rządowego projektu ustawy o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru oraz ochrony inwestorów na rynku finansowym, Sejm VIII kadencji, druk Sejm. nr 2812, s. 6.

[16] Uzasadnienie rządowego projektu ustawy o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru oraz ochrony inwestorów na rynku finansowym, Sejm VIII kadencji, druk Sejm. nr 2812, s. 6.

polskiego systemu prawnego domniemania zasady dematerializacji listu zastawnego należy ocenić pozytywnie. Zdematerializowana forma papierów wartościowych zwiększa bowiem elastyczność ich emisji.

5. Dematerializacja listów zastawnych a wykorzystanie technologii *blockchain*

W piśmiennictwie, na tle zagadnienia dematerializacji papierów wartościowych zaczynają być formułowane dalej idące postulaty *de lege ferenda* tokenizacji obligacji (Czaplicki 2022, s. 85–91). Podnoszone postulaty, z racji odpowiedniego stosowania przepisów ustawy z dnia 15 stycznia 2015 r. o obligacjach (Dz.U. 2024 poz. 708), mogą być odnoszone również do formy listów zastawnych, dlatego też zasadne jest rozważenie dopuszczalności wykorzystania możliwości technologii rozproszonych rejestrów do organizacji obrotu listami zastawnymi.

Technologia *blockchain* jeszcze do niedawna była kojarzona wyłącznie z rynkiem walut cyfrowych. Zachodzące zmiany technologiczne i coraz szersze wykorzystanie tych rozwiązań skłaniają do podjęcia dyskusji na tle możliwości tokenizacji obrotu papierami wartościowymi. W odniesieniu do zagadnienia dematerializacji listów zastawnych postulaty te są warte uwagi, przy czym tokenizacja obligacji, a także idąca za tym ewentualna tokenizacja listów zastawnych, wymaga przede wszystkim wprowadzenia systemowych zmian regulacyjnych, dostosowujących obecne zasady emisji do wymagań, jakie stawia zastosowanie technologii łańcucha bloków. Podkreślenia wymaga, że list zastawny podlega zarejestrowaniu w depozycie papierów wartościowych prowadzonym zgodnie z przepisami ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi. Emitent występuje z wnioskiem do KDPW o zawarcie umowy, której przedmiotem jest rejestracja listów zastawnych w depozycie papierów wartościowych. Rejestracja listów zastawnych następuje w trybie określonym w Szczegółowych Zasadach Działania KDPW (KDPW 2017). W konsekwencji powyższego, obowiązek zarejestrowania listu zastawnego w depozycie papierów wartościowych *de facto* uniemożliwia tokenizację listu zastawnego i jego funkcjonowanie w ramach systemu rejestrów rozproszonych, a nie scentralizowanego i nadzorowanego rejestru (Czaplicki 2022, s. 88). Potencjalna tokenizacja listów zastawnych wymagałaby także dostosowania technologii stosowanych przez KDPW do funkcjonowania w nowych realiach obrotu papierami wartościowymi (Czaplicki 2022, s. 90 i n.). Postulowane w piśmiennictwie zmiany dotyczące tokenizacji papierów wartościowych nie mogą być uzasadniane wyłącznie popularnością tego zjawiska i wykorzystania technologii *blockchain* w obrocie gospodarczym, lecz wymagają pogłębionej analizy, zwłaszcza możliwości technologicznych, dla zapewnienia bezpieczeństwa obrotu tokenami inkorporującymi papiery wartościowe. Należy mieć na względzie, że technologia rozproszonych rejestrów, mając postać wirtualną, może funkcjonować ponad granicami państw, stanowiąc wyzwania regulacyjne dla prawodawcy i konieczność przyjęcia spójnych ram regulacyjnych (Sousa 2023, s. 416).

Jakkolwiek korzyści płynące z inkorporowania papierów wartościowych w formie zdematerializowanej zdają się przewyższać dostrzegalne ryzyka, to jednak nie może ujść uwadze, że dematerializacja nie jest rozwiązaniem inkorporowania papierów wartościowych całkowicie pozbawionym ryzyk. Dematerializacja listów zastawnych wiąże się bowiem z nowymi ryzykami, eksponując przede wszystkim bezpieczeństwo obrotu na podwyższone ryzyko awarii systemów komputerowych. Odnosząc się natomiast do formułowanych postulatów *de lege ferenda* tokenizacji obrotu papierami wartościowymi (Czaplicki 2022, s. 85–91), w kontekście potencjalnego zastosowania technologii *blockchain* w piśmiennictwie trafnie akcentuje się również podatność tej technologii na luki w zabezpieczeniach (Sousa 2023, s. 416). Nie można także pomijać ryzyka możliwości popełnienia na rynku kapitałowym przestępstw z wykorzystaniem nowoczesnych technologii informatycznych (tzw. cyberprzestępczości)[17].

Podsumowanie

Zagadnienie dematerializacji papierów wartościowych charakteryzuje się dynamiką zmian regulacyjnych, na którą nakłada rozwój technologii łańcucha bloków i zgłaszanych w piśmiennictwie postulatów wprowadzenia tokenizacji papierów wartościowych. Problematyka dematerializacji listów zastawnych ma tym samym charakter wieloaspektowy. Funkcjonowanie w zmieniających się realiach obrotu papierami wartościowymi wymaga dostosowania do ewoluujących warunków obrotu na rynku kapitałowym, ze szczególnym uwzględnieniem ryzyk, jakie wiążą się z dematerializacją listów zastawnych. Poczynione w artykule rozważania i weryfikacja postawionych na wstępie hipotez prowadzą do wniosku, że wprowadzenie do polskiego systemu prawnego dematerializacji listu zastawnego i związanego z nią domniemania zasady dematerializacji, należy ocenić pozytywnie. Dematerializacja listów zastawnych sprzyja elastyczności emisji tych papierów wartościowych, zarazem zwiększając bezpieczeństwo obrotu przez niwelowanie ryzyk jakie niesie za sobą tradycyjna, dokumentowa forma papieru wartościowego.

W kontekście przyznania prymatu zasadzie dematerializacji listów zastawnych uzasadnione staje się pytanie o kierunki zachodzących zmian w zakresie formy tych papierów wartościowych. Niewątpliwie rozwój technologii komputerowej, w tym postęp w zakresie rozwoju technologii łańcucha bloków, skłania do podjęcia dyskusji na tle możliwości tokenizacji papierów wartościowych. Tokenizacja zakładająca odzwierciedlenie papierów wartościowych w cyfrowej formie, zapisanych w wirtualnych, rozproszonych rejestrach wymaga wprowadzenia systemowych zmian regulacyjnych, dostosowujących obecne zasady emisji papierów wartościowych do wymagań technologicznych jakie pociąga za sobą zastosowanie technologii łańcucha bloków. Na tle tych zagadnień

[17] Por. Romanowski 2016, s. 115; Dybiński 2016, s. 1317. Jakkolwiek brak legalnej definicji „cyberprzestępczości", to jednak w piśmiennictwie trafnie pojęcie to odnosi się do wszelkich działań o charakterze przestępczym podejmowanych: „przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych, jak również nieprawidłowemu ich wykorzystywaniu", zob. Gryszczyńska i Klawikowski 2022, s. 46.

nie można tracić z pola widzenia realiów funkcjonowania rynku kapitałowego i potrzeby zapewnienia przede wszystkim bezpieczeństwa i pewności tego obrotu. Dematerializacja listów zastawnych, jakkolwiek stanowi bezpieczne rozwiązanie inkorporowania papierów wartościowych, to jednak nie jest rozwiązaniem całkowicie pozbawionym ryzyk, zwłaszcza możliwości popełnienia na rynku kapitałowym przestępstw z wykorzystaniem nowoczesnych technologii informatycznych.

Bibliografia

Bellinger D. (1994), *Die Hypothekenbanken und der Pfandbrief in Deutschland*, VDH, Fritz Knapp Verlag, Frankfurt/Main.

Chłopecki A. (1995), *Obrót papierami wartościowymi na rynku kapitałowym (I)*, „Przegląd Prawa Handlowego", nr 8.

Chłopecki A. (2006), *Dematerializacja i obrót papierami wartościowymi (instrumentami finansowymi)*, [w:] *System prawa prywatnego*, t. 19, *Prawo papierów wartościowych*, red. A. Szumański, Warszawa.

Czaplicki P. (2022), *Tokenizacja obligacji – uwagi na tle art. 8 ust. 2 ustawy z dnia 15 stycznia 2015 r. o obligacjach*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny", nr 7(11).

Dybiński J. (2016), *Zagadnienia ogólne ochrony inwestora na rynku instrumentów finansowych*, [w:] *System Prawa Handlowego*, t. 4, *Prawo instrumentów finansowych*, red. M. Stec, Warszawa.

Dżuryk A. (2018), *List zastawny jako przykład bezpiecznego hipotecznego instrumentu finansowego*, „Zarządzanie i Finanse Journal of Management and Finance", Vol. 16, No. 4/1.

Gryszczyńska A., Klawikowski A. (2022), *Nowe wyzwania dla Prokuratury związane ze zwalczaniem przestępczości gospodarczej i cyberprzestępczości*, „Prokuratura i Prawo", nr 7–8.

Jastrzębski J. (2009), *Pojęcie papieru wartościowego wobec dematerializacji*, Warszawa.

Kanigowski K. (2019), *List zastawny. 250 lat historii,* Centrum Prawa Bankowego i Informacji, Warszawa.

Kaszubski R.W., Olszak M. (2000), *Bank hipoteczny. Zagadnienia prawne*, Warszawa.

KDPW (2017), Szczegółowe Zasady Działania Krajowego Depozytu Papierów Wartościowych przyjęte uchwałą Zarządu Krajowego Depozytu Papierów Wartościowych S.A. Nr 655/17 z dnia 28 września 2017 r. ze zm.

Mekiński M. (2001), *Regulacje nadzorcze w ustawie o listach zastawnych i bankach hipotecznych, cz. I*, „Glosa", nr 12.

Michalski M. (1999), [w:] L. Sobolewski (red.), *Prawo o publicznym obrocie papierami wartościowymi. Komentarz*, Warszawa.

Michalski M. (2006), *Bankowe papiery wartościowe*, [w:] *System prawa prywatnego*, t. 19, *Prawo papierów wartościowych*, red. A. Szumański, Warszawa.

Piech K. (red.) (2016), *Leksykon pojęć na temat technologii blockchain i kryptowalut*, Warszawa 2016, https://www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf/77392774-1180-79ab-4dd5-089ffab37602 (dostęp 23.04.2024).

Pieter J. (1975), *Zarys metodologii pracy naukowej*, Warszawa.

Pietrasik A., Laskowski A. (2001), *Historia i współczesność długoterminowego kredytu hipotecznego w Polsce*, Warszawa.

Romanowski M. (2016), *Zagadnienia ogólne papierów wartościowych*, [w:] *System prawa prywatnego*, t. 18, *Prawo papierów wartościowych*, red. A. Szumański, Warszawa.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz.U.UE L z 2014 r. Nr 257, str. 1 z późn. zm.).

Sattler F. (2019), *Von den Anfängen bus zum Boom der Hypothekenbankem (1769 bis 1914)*, [w:] F. Sattler, *Der Pfandbrief 1769–2019. Von der preuβischen Finanzinnovation zur Covered Bond Benchmark*, Stuttgart.

Sousa M.J. (2023), *Blockchain as a driver for transformations in the public sector*, „Policy Design and Practice", nr 6(4).

Sójka T., Godlewski M. (2022), *Art. 7*, [w:] *Obrót instrumentami finansowymi. Komentarz*, red. T. Sójka, Warszawa, Lex 2022.

Serzysko A. (2023), *DLT Pilot Regime (technologia rozproszonego rejestru) w sektorze finansowym w postanowieniach ustawy o rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku*, LEX/el..

Szczygieł J. (2017), *Trwały nośnik w obrocie konsumenckim*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny", nr 3(6).

Świderska-Iwicka M. (1995), *Depozyt papierów wartościowych*, „Przegląd Prawa Handlowego", nr 9.

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2023 poz. 1610 z późn. zm.).

Ustawa z dnia 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych (Dz.U. 2023 poz. 110).

Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U. 2022 poz. 1500 z późn. zm.).

Ustawa z dnia 15 stycznia 2015 r. o obligacjach (Dz.U. 2022 poz. 2244 z późn. zm.).

Ustawa z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku (Dz.U. poz. 2243 z późn. zm.).

Ustawa z dnia 7 kwietnia 2022 r. o zmianie ustawy o listach zastawnych i bankach hipotecznych oraz niektórych innych ustaw (Dz.U. 2022, poz. 872).

Uzasadnienie rządowego projektu ustawy o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru oraz ochrony inwestorów na rynku finansowym, Sejm VIII kadencji, druk Sejm. nr 2812.

Uzasadnienie rządowego projektu ustawy o zmianie ustawy o listach zastawnych i bankach hipotecznych oraz niektórych innych ustaw, Sejm IX kadencji, druk Sejm. nr 2019.

DOI: 10.26354/bb.6.1.94.2024

Natalia Rosiak*
ORCID: 0009-0008-9193-674X
n.rosiak@lawarton.com

Wojciech Kapica**
ORCID: 0000-0001-5753-3164
w.kapica@lawarton.com

Etyka w świetle Rekomendacji Z Komisji Nadzoru Finansowego dotyczącej ładu wewnętrznego w bankach – uwagi *de lege lata* i *de lege ferenda*

Streszczenie

W artykule przedstawiono zagadnienia etyki bankowej, w szczególności zawarte w Rekomendacji Z. Dokonano porównania wartości etycznych zawartych w Corporate governance principles for banks, Wytycznych EBA w sprawie zarządzania wewnętrznego oraz w Rekomendacji Z. Następnie sformułowano wnioski *de lege lata* i *de lege ferenda*. Osiągnięcie wyznaczonego celu wymagało wykorzystania metod badawczych, takich jak obserwacji naukowej opartej na przeglądzie dostępnej literatury, publikacji i materiałów źródłowych z sektora bankowego wraz z analizą i wnioskowaniem.

Słowa kluczowe: Rekomendacja Z Komisji Nadzoru Finansowego, Corporate governance principles for banks, Wytyczne EBA w sprawie zarządzania wewnętrznego, etyka, etyka bankowa, ład korporacyjny, kodeks etyczny, kultura ryzyka, pracownicy banku, bank

Kody JEL: K23

* Natalia Rosiak – adwokat w kancelarii Lawarton.
** Wojciech Kapica – radca prawny w kancelarii Lawarton.

Ethics in light of Recommendation Z of the Financial Supervision Commission on internal governance in banks – *de lege lata* and *de lege ferenda* remarks

Abstract

The article presents the issues of banking ethics, in particular those included in Recommendation Z. A comparison of ethical values contained in Corporate governance principles for banks, the EBA Guidelines in the field of internal management and in Recommendation Z was made. Then, *de lega lata* and *de lege ferenda* conclusions were formulated. Achieving the set goal required the use of research methods such as scientific observation based on a review of the available literature, publications and source materials from the banking sector, along with analysis and inference.

Keywords: Recommendation Z of the Polish Financial Supervision Authority, Corporate governance principles for banks, EBA Guidelines on internal governance, ethics, banking ethics, corporate governance, code of ethics, risk culture, bank employees

JEL Codes: K23

Wstęp

Celem niniejszego opracowania jest sformułowanie wniosków *de lega lata* i *de lege ferenda* odnośnie do etyki w świetle Rekomendacji Z Komisji Nadzoru Finansowego z 2020 roku dotyczącej zasad ładu wewnętrznego w bankach (dalej: **„Rekomendacja Z"**). Aby zrealizować ten cel w artykule przedstawiono pojęcie etyki, w tym etyki bankowej. Zaprezentowano podstawowe zagadnienia z tego zakresu, zaczerpnięte zarówno z literatury przedmiotu, jak i praktyki bankowej, dokonując przeglądu wartości etycznych zawartych w Corporate governance principles for banks wydanych w 2015 roku przez Bazylejski Komitet Nadzoru Bankowego (dalej: **„Corporate governance principles for banks"**) oraz Wytycznych w sprawie zarządzania wewnętrznego zgodnego z dyrektywą (UE) 2019/2034 z dnia 22 listopada 2021 roku wydanych przez Europejski Urząd Nadzoru Bankowego (dalej: **„Wytyczne EBA w sprawie zarządzania wewnętrznego"**) oraz w Rekomendacji Z. Następnie dokonano porównania tych dokumentów i sformułowano wnioski *de lege lata* i *de lege ferenda*. Realizacja postawionego celu trwała miesiąc i wymagała zastosowania następujących metod badawczych: obserwacji naukowej opartej na przeglądzie dostępnej literatury, publikacji i materiałów źródłowych z sektora bankowego wraz z analizą i wnioskowaniem.

1. Etyka bankowa

W literaturze często podkreśla się, że definicja etyki nie jest łatwa do jednoznacznego określenia, co sprawia, że precyzyjne zdefiniowanie jej jest trudne. W piśmiennictwie zauważa się, że etyka działalności gospodarczej jest zbiorem zasad uczciwego i od-

powiedzialnego zachowania przedsiębiorców, zarówno w bezpośrednich relacjach, jak i w szerszym kontekście społecznym. W kontekście sektora bankowego, termin „etyczny" jest stosowany do opisania (Mizdrak, Pogodzińska-Mizdrak 2013, s. 54):

- stylu i atrybutu rzetelnej działalności bankowej,
- dookreślenia banku „tytularnie" jako banku mającego wpisane w kanony moralne i społeczne założenia do celów swojego działania.

W związku z tym, „każdy bank komercyjny może być nazwany etycznym, jeśli realizuje określone wartości i cele społeczne, a jego działalność odznacza się prawością, transparentnością formalnoprawną i finansową, uczciwością, rzetelnością, lojalnością względem klientów, poszanowaniem praw pracowniczych itp. Innymi słowy, taki bank działa w sposób etyczny i jest otwarty na pewne inicjatywy społeczne. Natomiast tytułowy »bank etyczny« (inaczej: bank alternatywny lub bank misyjny) jest to instytucja finansowa, która została powołana i ufundowana kierunkowo na realizację wymienionych wyżej wartości i rzeczywiście je realizuje w swoim regionie, mając stale na uwadze dobro ludzi, instytucji oraz interes społeczny" (Mizdrak, Pogodzińska-Mizdrak 2013, s. 54).

Z powodu braku ustalonego katalogu działań etycznych lub nieetycznych, podejmowane są próby kwalifikacji danych zachowań jako etycznych bądź nie w ramach np. kodeksów etyki. Mimo to, nadal mogą pojawiać się nowe zachowania i działania, które nie zawsze są możliwe do jednoznacznej kategoryzacji (Komierzyńska-Orlińska 2019, s. 62). Banki nieuchronnie napotykają na nieetyczne dylematy, a często granica pomiędzy postępowaniem etycznym a nieetycznym bywa niejasna (Świeszczak, s. 189).

Postępowania niezgodne z zasadami etyki bankowej prędzej czy później zdyskredytują bank i podważą jego wiarygodność. Informacje przekazywane przez bank nie mogą być fałszywe. Każde przekłamanie lub niedopowiedzenie banku może spowodować, że wszystkie kolejne przekazy będą odbierane z dystansem i nieufnością. Informacje przekazywane przez bank muszą być prawdziwe i opierać się na faktach. Nawet jeśli odbiorca może nie zgodzić się z treścią przekazywanej przez bank informacji, nie będzie mógł mu zarzucić, że jest ona nieprawdziwa, co zapobiegnie nieodwracalnej utracie zaufania do banku (Macierzyński, Macierzyński 2014, s. 46).

Etyka w bankowości jest skoncentrowana wokół trzech obszarów (Gasparski 2004, s. 23–24):

- zasad etycznych transakcji dokonywanych na rynkach finansowych (dotyczy reguł, które panują na rynkach finansowych, np. każdy uczestnik transakcji na rynku finansowym powinien posiadać jednakowy dostęp do informacji),
- reguł budowania relacji z klientami (koncentracja na zbudowaniu relacji długoterminowych),
- dylematów osobistych osób zaangażowanych w dwa poprzednie obszary.

W ostatnich latach można zaobserwować zwiększenie nacisku na etykę w biznesie. Jednym z takich przykładów dla sektora bankowego stały się programy i kodeksy etyczne. Spośród licznych definicji kodeksów można przytoczyć tę zawartą w słow-

niku wyrazów obcych. Według autorów tego słownika: kodeks to: „zespół norm, reguł, zasad, przepisów dotyczących jakieś dziedziny, np. etyki" (Sobol 1996, s. 560). Należy zaznaczyć, że kodeks etyczny, będący albo odrębnym dokumentem, albo kluczowym elementem programu etycznego, przedstawia zbiór fundamentalnych zasad postępowania obowiązujących w organizacji lub standardów etycznych specyficznych dla danego zawodu. Z kolei program etyczny jest kompleksowym działaniem, którego celem jest ustanowienie etyki jako najważniejszego kryterium działania w firmie. Jako nieodzowny składnik takiego programu kodeks etyczny przyczynia się do kształtowania etycznej kultury organizacyjnej. Kodeksy etyczne są bądź jedynym – co dzieje się częściej – dokumentem określającym standardy zachowań w organizacji, bądź – co rzadziej – stanowią składnik programu etycznego tej organizacji. W tym drugim przypadku opracowywanie programu etycznego poprzedza prace nad kodeksem (Gasparski 2013, s. 235).

Eksperci zajmujący się opracowywaniem kodeksów etycznych podkreślają, że kluczowym elementem nie jest dokument kodeksu, ale proces jego tworzenia. Ten proces wspiera jednoczenie środowiska pracy i przyczynia się do rozwoju poczucia współodpowiedzialności za finalną wersję kodeksu, co jest niezwykle ważnym aspektem psychologicznym. Ogromne znaczenie mają tutaj wspólne wartości, które są fundamentem dla całego przedsięwzięcia. (Gasparski 2013, s. 236). Kluczowym składnikiem każdego programu etycznego jest kodeks etyczny, czyli zbiór zasad postępowania. Kiedy jest on skutecznie wdrożony i przestrzegany, przyczynia się do ograniczenia korupcji, oszustw finansowych oraz innych negatywnych zachowań. Pomaga również minimalizować przypadki konfliktu interesów. Efektem jest wzrost zaufania ze strony klientów, biznesowych partnerów i kontrahentów, a także zwiększenie autorytetu i lojalności pracowników, co w konsekwencji poprawia ogólną reputację organizacji (Gasparski 2013, s. 238). Skuteczny kodeks wzmacnia odpowiedzialność społeczną i wyjaśnia normy i wartości, których organizacja stara się przestrzegać. Ma charakter wizjonerski i transformacyjny, zapewniając wskazówki w trudnych okolicznościach. Nadaje ton organizacji i może być kluczowym dokumentem strategicznym firmy, na którym opierają się wszystkie decyzje (Stevens 2009, s. 14). Obowiązek etycznego postępowania dyrektorów, menedżerów i pracowników oraz obowiązek wydania kodeksu etyki jest obecnie uważany za ortodoksyjną praktykę ładu korporacyjnego w większości jurysdykcji (Keeper 2012, s. 2). Jednakże kodeks etyki może służyć jako kluczowy dokument strategiczny w organizacji lub może być po prostu dekoracją witryny – artefaktem, który sprawia, że organizacja wydaje się bardziej etyczna w oczach interesariuszy (Stevens 2009, s. 14).

„Mając na uwadze specyfikę banku jako instytucji zaufania społecznego, Związek Banków Polskich, instytucja zrzeszająca polskie banki, przyjął 18 kwietnia 2013 roku obowiązujący wszystkich swoich członków Kodeks Etyki Bankowej, zastępujący dotychczasowe Zasady Dobrej Praktyki Bankowej z 9 maja 2001 roku. Nowy dokument został znacząco poszerzony, dzięki czemu lepiej odpowiada nowym warunkom, w których funkcjonują instytucje finansowe. Sam fakt zmiany nazwy świadczy o znaczącej roli etyki w prowadzeniu działań przez instytucje finansowe. Bardzo dużo uwagi zwraca się na relacje z klientami, partnerami biznesowymi,

wzajemne stosunki pomiędzy bankami, ale również ze środowiskiem lokalnym" (Macierzyński, Macierzyński 2014, s. 49).

Kodeks Etyki Bankowej został opracowany w sposób klarowny i skondensowany. Ogólnie, ale zarazem wyraźnie, wskazano w nim wiele zasad, którymi powinny kierować się banki jako instytucje i pracownicy banków w relacjach z otoczeniem wewnętrznym i zewnętrznym. Termin „powinien" w różnych odmianach jest najczęściej występującym orzeczeniem czasownikowym (48 powtórzeń) w Kodeksie Etyki Bankowej. W ten sposób dokument ten dostarcza zestaw obowiązujących wzorców pożądanego przez normodawcę zachowania w formie pośredniej, powinnościowej, a nie bezpośredniej, nakazowej. Kodeks Etyki Bankowej dzieli się na: Część A. Kodeks Dobrych Praktyk Bankowych i Część B. Kodeks Etyki Pracownika Banku. Kluczową częścią Kodeksu Etyki Bankowej są postanowienia końcowe, które rekomendują organizowanie szkoleń dla pracowników banków w celu zapoznania ich z zasadami zawartymi w kodeksie, jak również nadzór nad ich przestrzeganiem (Czechowska, Zatoń, 2016, 123–124).

2. Etyka w ładzie wewnętrznym

Zgodnie z definicją opracowaną przez Giełdę Papierów Wartościowych w Warszawie, ład korporacyjny to zbiór zasad postępowania, skierowanych zarówno do organów spółek oraz członków tych organów, jak i do większościowych i mniejszościowych akcjonariuszy. Zasady ładu korporacyjnego odnoszą się do szeroko rozumianego zarządzania spółką.

Oprócz przepisów prawnych obowiązujących w danym kraju dobre praktyki ładu korporacyjnego stanowią ważny czynnik determinujący zachowanie organów spółek, członków tych organów oraz większościowych i mniejszościowych akcjonariuszy. Przy tworzeniu tych praktyk uczestniczą różnego rodzaju instytucje, zarówno rządowe, jak i quasirządowe, komitety powołane przez władze państwowe lub władze giełdowe, stowarzyszenia obejmujące przedstawicieli świata nauki i biznesu oraz stowarzyszenia dyrektorów. Dobre praktyki funkcjonują w ramach „miękkiego prawa"; nie są więc regulacjami stanowionymi przez państwo. Ich stosowanie przez uczestników rynku jest, formalnie biorąc, dobrowolne i przyjmuje formułę: „zastosuj albo wyjaśnij, dlaczego nie stosujesz": (*comply or explain*). Należy jednak zauważyć, że mimo braku mocy prawnej rekomendacje dotyczące dobrych praktyk są zbyt ważne i nie mogą być całkowicie ignorowane przez spółki i członków ich organów (Koładkiewicz 2013, s. 302).

Rekomendacja Z stanowi zbiór dobrych praktyk w zakresie zasad ładu wewnętrznego. Na ład wewnętrzny składają się w szczególności: system zarządzania bankiem, organizacja banku, zasady działania, uprawnienia, obowiązki i odpowiedzialność oraz wzajemne relacje rady nadzorczej, zarządu i osób pełniących kluczowe funkcje w banku. Ład wewnętrzny banków jest uregulowany poprzez:

- Ustawę z dnia 29 sierpnia 1997 roku Prawo bankowe (Dz. U. z 2023 r. poz. 2488),
- Rozporządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 8 czerwca 2021 roku, w sprawie systemu zarządzania ryzykiem i systemem kontroli wewnętrznej oraz polityki wynagrodzeń w bankach (Dz. U. z 2021 r. poz. 1045).

Poza aktami prawa powszechnie obowiązującego, ład wewnętrzny banków jest uregulowany poprzez akty „prawa miękkiego" takie jak:

- Dobre Praktyki Spółek Notowanych na GPW 2021, jeżeli bank jest spółką notowaną na Giełdzie Papierów Wartościowych,
- Zasady Ładu Korporacyjnego dla instytucji nadzorowanych wydane przez Komisję Nadzoru Finansowego.

Ponadto wybrane zagadnienia są przedmiotem innych Rekomendacji wydanych przez Komisję Nadzoru Finansowego:

- Rekomendacji H dotyczącej systemu kontroli wewnętrznej w bankach,
- Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach.

Dodatkowo, ład korporacyjny jest uregulowany w:

- Corporate governance principles for banks,
- Wytycznych EBA w sprawie zarządzania wewnętrznego.

Rekomendacja Z jest próbą zgromadzenia, usystematyzowania i ułożenia ogólnych zasad i dobrych praktyk w sektorze bankowym w jedną całość. Co prawda Rekomendacja Z nie jest źródłem prawa powszechnie obowiązującego, to pozwala podmiotom nadzorowanym poznać sposób interpretacji przepisów przez Komisję Nadzoru Finansowego, a co za tym idzie dostosować swoją działalność do jej wymogów. Postanowienia Rekomendacji Z powinny być traktowane jako uzupełniające przepisy ustaw i rozporządzeń oraz Corporate governance principles for banks, a także Wytycznych EBA w sprawie zarządzania wewnętrznego. Ponadto nie powinny być interpretowane w sposób z nimi sprzeczny.

Nie można zapominać, że kluczowym elementem *corporate governance* jest odpowiedzialność. Jest to podstawa, na której powinno się opierać budowanie bankowości. Chociaż przepisy prawne odgrywają ważną rolę w zapewnieniu przestrzegania tej zasady, to głównym motywatorem powinna być nie tyle obawa przed konsekwencjami, ile autentyczne poczucie odpowiedzialności za przyszłość banku oraz wszystkich zainteresowanych stron, których działalność banku dotyka. Biorąc pod uwagę specyfikę banków, w grę wchodzi nie tylko dobro bezpośrednich klientów i kontrahentów, ale również szeroko pojęte społeczeństwo, państwo, konkurenci oraz współpracownicy. Dlatego podkreśla się, że fundamentem dobrego władztwa korporacyjnego nie powinny być tylko normy prawne, ale przede wszystkim zasady etyczne. Idealnym podejściem jest zintegrowanie systemu władztwa korporacyjnego z kulturą etyczną instytucji. Przyjęte zasady i kodeksy etyki wspierają jej odpowiedzialne postawy względem interesariuszy, co jest kwintesencją władztwa korporacyjnego. Jednocześnie efektywny system *corporate governance* wspiera przestrzeganie przyjętego przez instytucję kodeksu etycznego i respektowanie obranych wartości (Marcinkowska 2014, s. 430–431).

3. Etyka w świetle Corporate governance principles for banks

W lipcu 2015 roku Bazylejski Komitet Nadzoru Bankowego (Basel Committee on Banking Supervision) opublikował zaktualizowaną wersję zasad ładu korporacyjnego dla banków Corporate governance principles for banks. Zmienione zasady zapewniają ramy, w ramach których banki i organy nadzoru powinny działać, aby osiągnąć solidne i przejrzyste zarządzanie ryzykiem i podejmowanie decyzji. Należyty ład korporacyjny banków może zwiększyć zaufanie społeczne oraz utrzymać bezpieczeństwo i solidność systemu.

3.1. Kodeks etyczny

Zgodnie z Corporate governance principles for banks, kierownictwo powinno opracować pisemny kodeks etyczny lub kodeks postępowania. Każdy z tych kodeksów ma na celu promowanie kultury uczciwości i odpowiedzialności w celu ochrony interesów klientów i akcjonariuszy.

Kodeks postępowania lub kodeks etyczny banku lub porównywalna polityka powinny określać dopuszczalne i niedopuszczalne zachowania.

a) Powinny wyraźnie zakazywać nielegalnej działalności, jak niewłaściwe zgłaszanie nieprawidłowości finansowych i nadużycia finansowe, przestępstwa gospodarcze, w tym oszustwa, naruszanie sankcji, pranie pieniędzy, praktyki antykonkurencyjne, przekupstwo i korupcja lub naruszanie praw konsumentów.
b) Powinny jasno określać, że od pracowników oczekuje się etycznego postępowania i wykonywania swojej pracy z umiejętnością, należytą starannością, a także przestrzegania przepisów prawa, regulacji i polityki firmy.

3.2. Kultura ryzyka

Rada[1] powinna nadawać *tone at the top* i nadzorować rolę kierownictwa we wspieraniu i utrzymywaniu solidnej kultury korporacyjnej i kultury ryzyka.

Podstawowym elementem dobrego zarządzania jest kultura korporacyjna polegająca na wzmacnianiu odpowiednich norm odpowiedzialnego i etycznego zachowania. Normy te są szczególnie istotne z punktu widzenia świadomości ryzyka w banku, zachowań związanych z podejmowaniem ryzyka i zarządzania ryzykiem (tj. „kultury ryzyka" banku).

[1] Ilekroć w Corporate governance principles for banks pojawia się określenie rada, należy przez to rozumieć organ, który nadzoruje zarządzanie. Struktura rady różni się w zależności od kraju. Użycie słowa „rada" w niniejszym dokumencie obejmuje różne modele krajowe, które istnieją i powinny być interpretowane zgodnie z prawem obowiązującym w każdej jurysdykcji.

W celu promowania zdrowej kultury korporacyjnej, rada powinna wzmocnić *tone at the top* poprzez:

a) ustalanie i przestrzeganie wartości korporacyjnych, które tworzą oczekiwania, że cała działalność powinna być prowadzona w sposób zgodny z prawem i etycznym, oraz nadzorowanie przestrzegania tych wartości przez kierownictwo wyższego szczebla i innych pracowników;
b) promowanie świadomości ryzyka w ramach silnej kultury ryzyka, poprzez przekazywanie oczekiwań rady, że nie popiera ona podejmowania nadmiernego ryzyka i że wszyscy pracownicy są odpowiedzialni za pomoc bankowi w działaniu w ramach ustalonego apetytu na ryzyko i limitów ryzyka;
c) potwierdzenie, że zostały lub zostaną podjęte odpowiednie kroki w celu informowania w całym banku o ustalonych przez niego wartościach korporacyjnych, standardach zawodowych lub kodeksach postępowania, wraz z politykami wspierającymi; oraz
d) potwierdzenie, że pracownicy, w tym kadra kierownicza wyższego szczebla, są świadomi, że za niedopuszczalne zachowania i wykroczenia będą następować odpowiednie działania dyscyplinarne lub inne.

3.3. Pracownicy

Wartości korporacyjne banku powinny uwzględniać kluczowe znaczenie terminowej i szczerej dyskusji oraz eskalacji problemów na wyższe szczeble organizacji.

a) Należy zachęcać pracowników banku do wyrażania w sposób poufny i bez ryzyka odwetu uzasadnionych obaw dotyczących nielegalnych, nieetycznych lub wątpliwych praktyk i umożliwiać im to. Można to ułatwić dzięki dobrze zakomunikowanej polityce oraz odpowiednim procedurom i procesom, zgodnym z prawem krajowym, które umożliwiają pracownikom zgłaszanie istotnych obaw oraz spostrzeżeń dotyczących wszelkich naruszeń w sposób poufny (np. zasady dotyczące sygnalistów).
b) Rada powinna sprawować nadzór nad mechanizmem polityki informowania o nieprawidłowościach i zapewniać, że kierownictwo wyższego szczebla zajmuje się uzasadnionymi kwestiami, które są zgłaszane. Rada powinna wziąć na siebie odpowiedzialność za zapewnienie, aby pracownicy, którzy zgłaszają obawy, byli chronieni przed szkodliwym traktowaniem lub represjami.
c) Rada ma obowiązek nadzorować i akceptować metody oraz osoby odpowiedzialne za badanie i rozstrzyganie kluczowych zagadnień. Powinny one być analizowane i rozwiązywane przez obiektywną i niezależną jednostkę wewnętrzną lub zewnętrzną, wyższy szczebel kierownictwa lub przez samą radę.

4. Etyka w świetle Wytycznych EBA w sprawie zarządzania wewnętrznego

Wytyczne w sprawie zarządzania wewnętrznego zgodnego z dyrektywą (UE) 2019/2034[2] zostały wydane na podstawie art. 16 rozporządzenia (UE) nr 1093/2010.[3]

W niniejszych wytycznych, zgodnie z art. 26 ust. 4 dyrektywy (UE) 2019/2034, szczegółowo określa się ustalenia, procesy oraz mechanizmy z zakresu zarządzania wewnętrznego, jakie powinny zostać wdrożone przez firmy inwestycyjne w ramach zastosowania postanowień tej dyrektywy w celu zapewnienia skutecznego i ostrożnego zarządzania takimi firmami.

Zgodnie z art. 4zf pkt 33 ustawy z dnia 29 lipca 2005 roku o obrocie instrumentami finansowymi[4], przez firmy inwestycyjne rozumie się dom maklerski, bank prowadzący działalność maklerską, zagraniczną firmę inwestycyjną prowadzącą działalność maklerską na terytorium Rzeczypospolitej Polskiej oraz zagraniczną osobę prawną z siedzibą na terytorium państwa innego niż państwo członkowskie, prowadzącą na terytorium Rzeczypospolitej Polskiej działalność maklerską.

4.1. Kodeks etyczny

Zgodnie z Wytycznymi EBA w sprawie zarządzania wewnętrznego, organ zarządzający jest odpowiedzialny za opracowanie i przyjęcie wysokich standardów etycznych i zawodowych, które powinien następnie nie tylko przestrzegać, ale i promować, biorąc pod uwagę szczególne potrzeby i specyfikę firm inwestycyjnych. Ma również za zadanie zapewnić, że te standardy zostaną wdrożone, na przykład poprzez stworzenie kodeksu postępowania lub podobnego dokumentu. Ponadto, organ zarządzający powinien monitorować, czy pracownicy przestrzegają ustalonych norm. W odpowiednich sytuacjach może on również zdecydować się na przyjęcie i wdrożenie standardów obowiązujących w całej grupie, do której należy firma inwestycyjna, lub wspólnych standardów wydanych przez stowarzyszenia lub inne stosowne organizacje.

Organ zarządzający powinien ustanowić jasną i udokumentowaną politykę w zakresie przestrzegania tych standardów. Polityka przyjęta przez organ zarządzający powinna:

a) przypominać pracownikom, że wszystkie działania firmy inwestycyjnej powinny być prowadzone zgodnie z obowiązującym prawem i przyjętymi przez nią wartościami;

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/2034 z dnia 27 listopada 2019 r. w sprawie nadzoru ostrożnościowego nad firmami inwestycyjnymi oraz zmieniająca dyrektywy 2002/87/WE, 2009/65/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE i 2014/65/UE.

[3] 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.U. L 331 z 15.12.2010, s. 12).

[4] Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U. z 2022 r. poz. 1500).

b) krzewić świadomość ryzyka, budując ugruntowaną kulturę ryzyka i komunikując oczekiwania organu zarządzającego, zgodnie z którymi działalność nie może wykraczać poza określony poziom gotowości do podejmowania ryzyka i limity określone przez firmę inwestycyjną, a zarazem wskazując odpowiednie obowiązki pracowników;
c) określać zasady oraz przedstawiać przykłady dopuszczalnych i niedopuszczalnych zachowań związanych w szczególności z nieprawidłowościami w sprawozdawczości finansowej i innymi uchybieniami w tej dziedzinie, przestępczością gospodarczą oraz finansową, w tym m.in. nadużyciami finansowymi, praniem pieniędzy i finansowaniem terroryzmu, praktykami monopolistycznymi, omijaniem sankcji finansowych, przekupstwem i korupcją, manipulacjami rynkowymi, nieprawidłowościami związanymi ze sprzedażą, innymi naruszeniami przepisów dotyczących ochrony konsumentów, przestępstwami podatkowymi, niezależnie od tego, czy zostały popełnione w sposób bezpośredni, czy pośredni, w tym w sposób niezgodny z prawem lub przy wykorzystaniu zakazanych systemów arbitrażu dywidendowego;
d) wyjaśniać, że oprócz spełnienia wymogów prawnych i regulacyjnych oraz zgodności z polityką wewnętrzną od pracowników oczekuje się uczciwego postępowania oraz wystarczająco umiejętnego i starannego wykonywania obowiązków; oraz
e) informować pracowników o potencjalnych wewnętrznych i zewnętrznych postępowaniach dyscyplinarnych, postępowaniach sądowych i sankcjach, jakimi mogą skutkować niewłaściwe postępowanie oraz niedopuszczalne zachowania.

Firmy inwestycyjne są zobowiązane do nadzorowania przestrzegania ustanowionych standardów oraz zapewnienia, by ich pracownicy byli z nimi dobrze zaznajomieni, na przykład poprzez organizowanie szkoleń. Należy powołać specjalną komórkę, która będzie odpowiedzialna za monitorowanie zgodności z kodeksem postępowania lub podobnym dokumentem, ocenę ewentualnych naruszeń oraz rozwijanie procedur postępowania w przypadku stwierdzenia niezgodności. Organ zarządzający powinien być na bieżąco informowany o wynikach tej działalności przez regularne sprawozdania.

4.2. Kultura ryzyka

Wdrożone standardy mają na celu umocnienie zasad zarządzania wewnątrz instytucji i zredukowanie ryzyka, przed którym stoi firma inwestycyjna, zwłaszcza w zakresie ryzyka operacyjnego oraz ryzyka utraty reputacji. Oba te czynniki mogą negatywnie wpłynąć na rentowność i stabilność firmy, prowadząc do możliwych kar pieniężnych, kosztów związanych z postępowaniami sądowymi, ograniczeń wprowadzonych przez właściwe organy, innych negatywnych konsekwencji finansowych i karnych, a także do spadku wartości marki i zaufania ze strony konsumentów.

Polityka przyjęta przez organ zarządzający powinna krzewić świadomość ryzyka, budując ugruntowaną kulturę ryzyka i komunikując oczekiwania organu zarządzającego, zgodnie z którymi działalność nie może wykraczać poza określony poziom

gotowości do podejmowania ryzyka i limity określone przez firmę inwestycyjną, a zarazem wskazując odpowiednie obowiązki pracowników.

Wytyczne EBA w sprawie zarządzania wewnętrznego poświęcają dużo miejsca kulturze ryzyka. Wskazują, że firmy inwestycyjne powinny rozwijać kulturę ryzyka przez wdrażanie polityki, komunikację i szkolenia dla pracowników na temat swojej działalności, strategii i profilu ryzyka, a także dostosować komunikację i szkolenia dla pracowników w celu uwzględnienia obowiązków tych pracowników w zakresie podejmowania ryzyka i zarządzania nim.

4.3. Pracownicy

Firmy inwestycyjne mają obowiązek zapewnienia równego traktowania swoich pracowników, bez względu na ich płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, przekonania religijne lub światopoglądowe, poglądy polityczne lub wszelkie inne, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek czy orientację seksualną.

Polityka firm inwestycyjnych powinna promować neutralność płciową, obejmując takie aspekty, jak: wynagrodzenia, procesy rekrutacyjne, awans zawodowy, plany sukcesji, dostęp do szkoleń oraz szanse aplikowania na otwarte pozycje przez wewnętrzne rekrutacje. Takie instytucje są zobowiązane do zapewnienia równych możliwości rozwoju kariery dla wszystkich pracowników, niezależnie od płci, starając się jednocześnie zwiększyć udział reprezentacji mniejszościowej płci na stanowiska w organie zarządzającym oraz w grupie personelu mającej kompetencje kierownicze, zgodnie z rozporządzeniem delegowanym Komisji (regulacyjne standardy techniczne w zakresie ustalania kategorii pracowników). Firmy inwestycyjne powinny także analizować tendencje związane z różnicami w wynagrodzeniach między płciami. W firmach inwestycyjnych zatrudniających co najmniej 50 osób taka analiza powinna być przeprowadzana oddzielnie dla różnych kategorii pracowników (z wyłączeniem członków organu zarządzającego), członków organu zarządzającego w ramach jego funkcji zarządczej, członków organu zarządzającego w ramach jego funkcji nadzorczej oraz pozostałych pracowników. Ponadto instytucje powinny opracować procedury ułatwiające reintegrację osób wracających z urlopów macierzyńskich, ojcowskich lub wychowawczych.

5. Etyka w świetle Rekomendacji Z

Komisja Nadzoru Finansowego, kontynuując politykę nadzorczą w zakresie należytej organizacji banków w obszarze szeroko rozumianego zarządzania zgodnością w dniu 9 października 2020 roku, opublikowała Rekomendację Z.

Rekomendacja Z stanowi zbiór dobrych praktyk w zakresie zasad ładu wewnętrznego. Ma na celu upowszechnienie dobrych praktyk oraz przeciwdziałanie stosowaniu przez banki, w zakresie objętym Rekomendacją Z, nieprawidłowych praktyk

zwiększających ryzyko ich działalności, a w konsekwencji zwiększenie odporności tych instytucji na trudne warunki rynkowe i tym samym wzrost stabilności sektora finansowego.

5.1. Kodeks etyki

Zgodnie z Rekomendacją Z, w banku powinny obowiązywać sporządzone w formie pisemnej zasady etyki. Wymagają one przyjęcia przez zarząd i zatwierdzenia przez radę nadzorczą. Określają normy i standardy etyczne dotyczące zachowań członków organów i pracowników banku, jak również innych osób, za pośrednictwem których bank prowadzi swoją działalność.

Zarząd ma również obowiązek regularnie dokonywać okresowej weryfikacji i oceny przestrzegania zasad etyki, aby móc je dostosować do ewoluujących warunków zarówno wewnątrz banku, jak i w jego otoczeniu. O wynikach przeprowadzonej oceny zarząd banku powinien, nie rzadziej niż raz w roku, informować radę nadzorczą.

5.2. Kultura ryzyka

Fundamentem dla budowania skutecznego ładu wewnętrznego w banku są wartości, którymi bank kieruje się w swojej działalności. Opracowane zasady etyki, opierające się na wyznaczonych wartościach i utrzymujące wysoki poziom standardów etycznych oraz zawodowych, powinny promować wśród pracowników banku postawy charakteryzujące się odpowiedzialnością i etycznym zachowaniem. To zadanie nabiera szczególnej wagi, gdy chodzi o zwiększenie świadomości pracowników banku o istotności ryzyka w działalności instytucji, jak również o zasadach podejmowania ryzyka i jego zarządzania, co jest znane jako tzw. kultura ryzyka. Wysokie normy etyczne i zawodowe powinny jednoznacznie wskazywać, jakie zachowania czy standardy postępowania są pożądane, a jakie nieakceptowane.

Komisja Nadzoru Finansowego w Rekomendacji Z podkreśla szczególną rolę zarządu w promowaniu zasad etycznych i zawodowych w banku. Zarząd banku powinien aktywnie promować ustanowione wysokie standardy etyczne i zawodowe, szczególnie podkreślając świadomość znaczenia ryzyka w działalności prowadzonej przez bank oraz kultury ryzyka.

6. Porównanie ujęć etyki

Porównując zawartość Corporate governance principles for banks, Wytycznych EBA w sprawie zarządzania wewnętrzenego oraz Rekomendacji Z, pod kątem ujęcia w nich kwestii etycznych, na pierwszy plan wysuwa się bardzo lakoniczne podejście do pojęcia etyki w Rekomendacji Z. Poświęcono mu najmniej miejsca. W zasadzie ograniczono się jedynie do potrzeby sporządzenia zasad etycznych. Tymczasem analiza zawartości Corporate governance principles for banks oraz Wytycznych EBA w sprawie zarządza-

nia wewnętrznego, pod kątem ujęć etyki, pozwala stwierdzić, że zarówno struktura, jak i treść dokumentów wykazują znaczne podobieństwo. Oba te dokumenty poświęcają etyce dużo więcej miejsca niż Rekomendacja Z. Wskazują, co w szczególności powinno się znaleźć w kodeksach etycznych. Przedstawiają, jakie zachowania pracowników są promowane, a jakie uznawane za naganne. Rekomendacja Z, oprócz potrzeby sporządzenia kodeksu etycznego, nie wymienia żadnej przykładowej jego zawartości. Na uznanie zasługuje fakt, że we wszystkich opisanych powyżej dokumentach podkreśla się rolę odpowiednich norm odpowiedzialnego i etycznego zachowania na kulturę ryzyka banku. Normy te mają szczególnie istotne znaczenie z punktu widzenia świadomości ryzyka w banku, zachowań związanych z podejmowaniem ryzyka i zarządzania ryzykiem. Kultura ryzyka jest pojęciem trudnym do zdefiniowania. W literaturze brak jest jednolitego ujęcia kultury ryzyka. Kultura ryzyka definiowana jest jako kategoria opisująca wartości, przekonania, postawy i wiedzę o ryzyku, podzielane przez daną grupę (pracownicy, kadra menedżerska, klienci, nadzorcy, regulatorzy) (Kasiewicz, Kurliński 2018, s. 41). W Rekomendacji Z temat kultury ryzyka w bankach jest tematem, który nie został poddany dogłębnej analizie. Ponadto w Rekomendacji Z brak jest powiązania etyki z kulturą ryzyka, które to powiązanie jest bardzo widoczne zarówno w Corporate governance principles for banks oraz w Wytycznych EBA w sprawie zarządzania wewnętrznego. Najpełniej kultura ryzyka opisana jest w Wytycznych EBA w sprawie zarządzania wewnętrznego. Akcentują one konieczność promowania postaw pracowników wszystkich szczebli, w celu wypracowania ich zachowania względem ryzyka.

Kwestie dotyczące stosunków między bankiem a jego pracownikami stanowią kolejną kwestię, która odróżnia Rekomendację Z od pozostałych dwóch opisanych dokumentów. Corporate governance principles for banks oraz Wytyczne EBA w sprawie zarządzania wewnętrznego zawierają duży obszar tematyczny dotyczący uprawnień pracowniczych. To powoduje, że dokumenty te nie są odbierane jako narzędzia dominacji lub kontroli nad pracownikami. Zamiast tego można w nich zaobserwować podejście oparte na partnerstwie. Pozycja pracowników została w nich wyraźnie wzmocniona. Na szczególną uwagę zasługują Corporate governance principles for banks w zakresie, w którym podkreślają istotną rolę zasad umożliwiających pracownikom zgłaszanie w sposób poufny istotnych obaw oraz spostrzeżeń dotyczących wszelkich naruszeń. Natomiast w Wytycznych EBA w sprawie zarządzania wewnętrznego podkreślono zobowiązanie do zapewnienia równych szans rozwoju kariery dla wszystkich pracowników, niezależnie od ich płci, a także starania w kierunku polepszenia wskaźnika reprezentacji mniejszościowej płci na stanowiskach w organie zarządzającym, a także w grupie personelu mającej kompetencje kierownicze. Tymczasem w Rekomendacji Z nie wspomniano o żadnych uprawnieniach pracowniczych, skupiając się jedynie na ich obowiązkach względem banku.

7. Wnioski *de lege ferenda* / Zakończenie

W piśmiennictwie wskazuje się, że autentyczne zaangażowanie się zespołu pracowników w kwestie etyczności firmy i kultury pracy nie powinno mieć charakteru przypadkowego, lecz stanowić pochodną udziału najwyższego kierownictwa

w projektowaniu programu etycznego korporacji. Istotne są tu wola i zaangażowanie kierownictwa w tworzenie systemu wspierającego kształtowanie etycznej substancji organizacji (Gasparski 2013, s. 236). Powszechnie zwraca się uwagę, że najczęściej przedstawiany obszar tematyczny zawarty w kodeksach dotyczy pracowników. Często ciężar odpowiedzialności za kulturę etyczną firmy, jej wizerunek i relacje zewnętrzne z interesariuszami spoczywa przede wszystkim na pracownikach. Pojawia się także pogląd o negatywnym wpływie kodeksów etyki na pracowników z powodu hierarchicznego języka, autorytarnego tonu i dyscyplinujących treści wpływających na to, że są odbierane jako instrumenty dominacji i kontroli przez zarząd firmy (Czechowska, Zatoń 2016, s. 118). Kodeksy etyczne mogą służyć jako podstawowe dokumenty, które dają członkom organizacji poczucie wspólnych wartości i zaangażowania w realizację celów etycznych. Szereg badań dostarczyło dowodów na to, że skutecznie zniechęcają do zachowań pozbawionych skrupułów, jednakże muszą być skutecznie przekazywane i wspierane przez kadrę kierowniczą. Dobra komunikacja jest pierwszym warunkiem skuteczności (Stevens 2009, s. 15). Banki, działając na zasadach wysokich standardów etycznych, powinny równie wysokie standardy stosować w relacjach pracowniczych, podkreślając ich znaczenie dla całej organizacji. Z uwagi na szczególną rolę banków w gospodarce, przyjmuje się, że ciąży na nich większe zobowiązanie do podejmowania działań społecznie odpowiedzialnych niż na typowych przedsiębiorcach ze sfery gospodarki realnej. W swojej działalności powinny uwzględniać kontekst społeczny, kontekst środowiska naturalnego oraz kontekst etyczny właśnie (Korenik 2013, s. 308).

Biorąc pod uwagę powyższe, kodeksy etyczne, będące odzwierciedleniem całych programów etycznych, powinny zapewniać równowagę pomiędzy powinnościami pracowników i pracodawców. Ponadto, oprócz obowiązków nakładanych na pracowników powinny zawierać przysługujące im uprawnienia. Kierownictwo w bankach tworząc program etyczny, a w jego ramach kodeksy etyczne, powinno sięgnąć do Rekomendacji Z. Rekomendacja ta jednak w sposób bardzo zdawkowy podchodzi do pojęcia etyki w bankach. W ujęciu etyki tylko dwukrotnie wspomina o pracownikach i to tylko w odniesieniu do nałożonych na nich obowiązków. Rekomendacja Z milczy na temat uprawnień czy szczególnej roli pracowników w banku. Tymczasem akcentowanie praw pracowniczych przyczynia się do zniwelowania nierówności w relacjach między kadrą zarządzającą banków a pracownikami. Skutkuje to poprawą wewnętrznych relacji bankowych, z jasno określonymi uprawnieniami pracowników i zakresem ich odpowiedzialności, co powinno mieć korzystny wpływ na etyczne i uczciwe podejście do klientów, odzwierciedlając rolę banku jako instytucji cieszącej się zaufaniem społecznym. Sektor bankowy powinien charakteryzować się wyjątkowym naciskiem na wzajemne zaufanie pomiędzy pracownikami a pracodawcami. Powinno ono być kluczowym elementem jego funkcjonowania. To zaufanie powinno być budowane na przestrzeganiu prawa, zrozumieniu i poszanowaniu wspólnych interesów zarówno przez pracowników, jak i pracodawców.

Pracownik, nie będący istotą doskonałą, wnosi do sektora bankowego dodatkowy element ryzyka, znanego jako ryzyko operacyjne. Ostatnio w świecie finansowym zaczęto przywiązywać do niego równie dużą wagę, jak do tradycyjnie rozpoznawanych

ryzyk bankowych, jak ryzyko kredytowe, ryzyko płynności, ryzyko stóp procentowych czy ryzyko walutowe, które mogą wpłynąć na osiągane przez bank wyniki finansowe. W związku z tym, przestrzeganie przez pracowników norm prawnych i etycznych ściśle wiąże się z kondycją finansową banku (Lipiński 2008, s. 93). Dlatego też zagadnienia dotyczące pracowniczych praw i obowiązków z perspektywy etycznej nie powinny być traktowane jako poboczne zagadnienia wymagające regulacji, lecz jako fundamentalne aspekty, które są istotne dla funkcjonowania ekonomii bankowej.

Rekomendacja Z powinna powiązać etykę z kulturą ryzyka. Nie można bowiem zapominać, że praktycznie każda aktywność banku będzie immanentnie związana z czynnikami generującymi pewien poziom ryzyka. W konsekwencji istotne jest, aby promując wzorce zachowania nie zapominać, że ich podstawą będzie wiedza umożliwiająca odpowiednie zrozumienie ryzyka do zajmowanego stanowiska lub posiadanych uprawnień decyzyjnych. Rosnąca rola kultury ryzyka w bankach nie może dokonać się bez zmiany podejścia samego nadzorcy. W związku z tym Komisja Nadzoru Finansowego odgrywa znaczącą rolę w procesie kształtowania, oceny i ulepszania kultury ryzyka w bankach, co powinno znaleźć odzwierciedlenie w Rekomendacji Z.

Zarówno Corporate governance principles for banks, jak i Wytyczne EBA w sprawie zarządzania wewnętrznego odchodzą od formalizmu w zakresie etyki. Tymczasem Rekomendacja Z skupia się wyłącznie na aspektach formalnych, a nie na efektywności procesu. Takie podejście nie służy propagowaniu kultury etycznej w bankach. Samo posiadanie kodeksów etycznych nie jest gwarantem bezpieczeństwa banków. Dopiero odpowiednie podejście do kodeksów etycznych przez pracowników na wszystkich szczeblach hierarchii organizacyjnej może przynieść pożądany efekt. Dlatego Rekomendacja Z nie powinna tylko skupiać się na elementach formalnych, funkcjonujących w banku, ale akcentować konieczność promowania postaw pracowników wszystkich szczebli, w celu wypracowania wzorców ich zachowań. Na ostateczny kształt Rekomendacji Z powinny mieć wpływ zarówno uregulowania zawarte w przepisach krajowych, jak i w regulacjach unijnych. Rekomendacja Z powinna zawierać postanowienia doprecyzowujące oraz uzupełniające te regulacje, w szczególności w zakresie ujęcia w nich etyki. W związku z tym Rekomendacja Z powinna dostosować swoje postanowienia do tych zawartych w Corporate governance principles for banks oraz Wytycznych EBA w sprawie zarządzania wewnętrznego, w taki sposób, aby podmioty nadzorowane mogły lepiej poznać sposób postrzegania kwestii etycznych przez Komisję Nadzoru Finansowego.

Bibliografia

Bazylejski Komitet Nadzoru Bankowego, *Corporate governance principles for banks*, 2015 (lipiec), https://www.bis.org/bcbs/publ/d328.pdf (dostęp 10.03.2024).

Czechowska I.D., Zatoń W. (2016), *Struktura i zawartość kodeksów etyki instytucji bankowych*, „Prakseologia", t. 158(1).

Europejski Urząd Nadzoru Bankowego, *Wytyczne w sprawie zarządzania wewnętrznego zgodnego z dyrektywą (UE) 2019/2034* z 22 listopada 2021 roku (EBA/GL/2021/14), https://

www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/EBA-GL-2021-14%20Guidelines%20on%20internal%20governance%20under%20IFD/translations/1028060/GL%20on%20internal%20governance%20under%20IFD_PL_COR.pdf (dostęp 10.03.2024).

Gasparski W. (2004), *Uczciwość w świecie finansów*, Wyższa Szkoła Przedsiębiorczości i Zarządzania im. L. Koźmińskiego.

Gasparski W. (2013), *Kodeksy i programy etyczne*, [w:] W. Gasparski, *Biznes, etyka, odpowiedzialność*. Warszawa: Wydawnictwo Profesjonalne PWN.

Kasiewicz S., Kurkliński L. (2018), *Kultura ryzyka w polskim sektorze bankowym na tle tendencji światowych*, „Annales Universitatis Mariae Curie-Skłodowska, sectio H (Oeconomia)", Vol. 52, No. 3.

Keeper T. (2012), *Codes Of Ethics and Corporate Governance: A Study of New Zealand Listed Companies* (October 20, 2011). *Corporate Governance after the Financial Crisis*, 2012. Available at http://ssrn.com (dostęp 10.04.2024).

Koładkiewicz I. (2013), *Ład korporacyjny*, [w:] W. Gasparski, *Biznes, etyka, odpowiedzialność*. Warszawa: Wydawnictwo Profesjonalne PWN.

Komierzyńska-Orlińska E. (2019), *Etyka w działalności banków w perspektywie kryzysu finansowego lat 2007–2009,* „Przegląd Prawa Administracyjnego", (2).

Komisja Nadzoru Finansowego, *Rekomendacja Z*, Warszawa 2020 (październik), https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_Z_70998.pdf (dostęp: 10.03.2024).

Korenik D. (2013), *Znaczenie społecznej odpowiedzialności banku w teorii i praktyce bankowej*, „Zarządzanie i Finanse" nr 2, cz. 1.

Lipiński Cz. (2008), *Etyka w bankowości – dylematy pracownika bankowego,* „Annales. Etyka w życiu gospodarczym", vol. 11, nr 2.

Macierzyński W., Macierzyński M. (2014), *Etyka w public relations bankowym*, „Przedsiębiorczość i Zarządzanie", z. 4, cz. 1.

Marcinkowska M. (2014)*, Corporate Governance w bankach. Teoria i praktyka*. Łódź.

Mizdrak I., Pogodzińska-Mizdrak E. (2013), *Społeczna odpowiedzialność w działalności banków na przykładzie Banca Popolare Etica*, „Studia i Prace Kolegium Zarządzania i Finansów / Szkoła Główna Handlowa", z. 130.

Sobol E. (1996), *Słownik wyrazów obcych*. Warszawa: PWN.

Stevens B. (2009), *Corporate ethical codes as strategic documents: An analysis of success and failure*, EJBO *„Electronic Journal of Business Ethics and Organization Studies"*, 14(2), http://ejbo.jyu.fi (dostęp 10.04.2024).

Świeszczak M. (2016), *Reklamy bankowe a ich kontekst etyczny*, https://dspace.uni.lodz.pl/xmlui/bitstream/handle/11089/20270/%5b181%5d_201_Swieszczak.pdf?sequence=1&-isAllowed=y (dostęp 6.03.2024).

Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U. z 2022 r. poz. 1500).

Związek Banków Polskich, *Kodeks Etyki Bankowej* (*Zasady Dobrej Praktyki Bankowej),* Warszawa 2013 (kwiecień), www.zbp.pl/getmedia/c54fc557-0e78-48e2-a92b-1a601685dbc7/KEB_final_WZ (dostęp 10.03.2024).

Miscellanea

DOI: 10.26354/bb.7.1.94.2024

Stanisław Kasiewicz*
ORCID: 0000-0003-3758-5033
skasie@sgh.waw.pl

Jacek Woźniak**
ORCID: 0000-0001-7592-0109
jacekj.wozniak@wat.edu.pl

Syntetyczna ocena zarządzania ryzykiem w polskim sektorze bankowym w świetle badań ankietowych

Streszczenie

Niniejszy artykuł nawiązuje do wyników badania empirycznego sektora banków w Polsce przeprowadzonego w okresie marzec – kwiecień 2023 roku (Kasiewicz, Woźniak 2024). Zasadniczym celem badania było wskazanie, jak banki w Polsce podchodzą do kształtowania systemu zarządzania ryzykiem w warunkach cyfryzacji procesów i ocenić te działania w perspektywie 2035 roku. W badaniu zastosowano technikę badania ankietowego CAWI (ang. *Computer-Assisted Web Interview*) oraz technikę statystycznej analizy danych ilościowych. W artykule zaprezentowane są odpowiedzi udzielone wyłącznie przez przedstawicieli banków (N=127). W opracowaniu weryfikuje się hipotezę: Banki zdążą zmodernizować system zarządzania ryzykiem do stanu jego ewolucji w 2035 roku. W stosunku do monografii odniesiono się odmiennie do interpretacji i komentarza uzyskanych wyników. Generalny wniosek, jaki nasuwa się z badania to, że nadal banki są mocno zawansowane w rozwiązywa-

* Stanisław Kasiewicz – emerytowany profesor Szkoły Głównej Handlowej w Warszawie.
** Jacek Woźniak – doktor nauk społecznych w dyscyplinie Nauki o Zarządzaniu i Jakości, Wojskowa Akademia Techniczna w Warszawie.

niu bieżących problemów i dość odległe od zdecydowanego przejścia na wdrożenie nowego paradygmatu zarządzaniu ryzykiem.

Słowa kluczowe: bank cyfrowy, sektor bankowy, zarządzanie ryzykiem, cele, funkcje i etapy zarządzania ryzykiem

Kody JEL: G32, O33

Synthetic assessment of risk management in the Polish banking sector in the light of survey research

Abstract

This article refers to the result of an empirical study of the banking sector in Poland conducted between March and April 2023 (Kasiewicz, Woźniak 2024). The main objective of the study was to indicate how banks in Poland approach the development of the risk management system in the conditions of digitization of processes and to assess these activities in the perspective of 2035. The study used the CAWI (*Computer-Assisted Web Interview*) survey technique and the technique of statistical analysis of quantitative data. The article presents answers given only by bank representatives (N=127). The study verifies the hypothesis: Banks will manage to modernize the risk management system to the state of its evolution in 2035. In relation to the monograph, a different approach was made to the interpretation and commentary of the results obtained. The general conclusion that comes to mind from the survey is that banks are still well advanced in solving current problems and quite far from a decisive transition to the implementation of a new risk management paradigm.

Keywords: digital bank, banking sector, risk management, objectives, functions and stages of risk management

JEL Codes: G32, O33

Wstęp

Transformacja cyfrowa banków wymaga wielu ryzykownych przedsięwzięć. Ich powodzenie w dużym stopniu zależy od oceny stanu systemu zarządzania ryzykiem. Organy banków, konkurując m.in. w obszarze zarządzania ryzykiem, opracowują modele biznesowe i ambitne strategie, niewystarczająco uwzględniając ograniczenia rynkowe, finansowe, kadrowe, technologiczne czy kulturowe organizacji. Takie podejście już samo w sobie generuje ryzyko nieskuteczności tych strategii. Ponadto warto wyeksponować ograniczenia swobody opracowywania strategii wynikające z silnych uwarunkowań prawnych czy regulacji nadzorczych, co w pewnym stopniu prowadzi do upodabniania strategii głównych aktorów na rynku bankowym. Warto do tego dodać konsekwencje komplementarności, a nawet substytucji kompetencji (wiedzy, umiejętności, postaw) kadr bankowych i nowoczesnych technologii cyfrowych. W tym kontekście jeden z najważniejszych dylematów decydentów w bankach dotyczy tego: ***Czy aktualny system zarządzania ryzykiem jest adekwatny do cech i uwarunkowań towarzyszących konkurencji cyfrowej?*** Artykuł składa

się z dwóch zasadniczych części: (1) przedstawienia istoty banku cyfrowego, jego cech i wartości oraz (2) prezentacji wyników badania empirycznego dotyczącego systemu zarządzania ryzykiem w bankach, a także Wstępu i Podsumowania.

1. Istota banku cyfrowego, jego cechy i wartości

Wzmianki o bankowości cyfrowej w literaturze poświęconej działalności instytucji finansowych zamieszczano już w latach 60. XX wieku, gdy zaczęto wykorzystywać bankomaty i karty płatnicze. Pojawienie się Internetu w latach 80. XX w. dało zasadniczy impuls do rozwoju bankowości cyfrowej (Kelman 2016). Do 2020 r. zaszło wiele zmian w definiowaniu i operacjonalizacji tej formy bankowości oraz w ocenie jej oddziaływania na rynki finansowe. A proces ten nie sposób uznać za zakończony.

Miano banku cyfrowego przypisuje się podmiotowi, który wykorzystuje nowe lub rozwojowe technologie do świadczenia usług finansowych klientom, a wdraża innowacyjne zmiany wewnętrzne i zewnętrzne, w tym przede wszystkim w relacjach z klientami, aby zapewnić efektywniejsze zaspokojenie ich potrzeb (Ginovsky 2015). Inna wersja ujęcia istoty banku cyfrowego eksponuje okoliczność, że nowa technologia staje się nie tylko dodatkowym elementem, ale stanowi jego „jądro" funkcjonowania. Przejawia się to m.in. w tym, że klienci używają głównie mobilnych urządzeń do wykonywania operacji bankowych, w tym założenia rachunku czy otwarcia nowego konta oraz przeprowadzania rozliczeń, zakładania lokat, zaciągania kredytu, inwestowania w fundusze, zgłaszania reklamacji itd. Wszystkie te czynności są realizowane bez fizycznego kontaktu z placówką bankową czy pracownikiem banku (Barquin i Vinayak 2016). Szczególnie aktywne w tym obszarze są młodsze generacje klientów, dla których bankowość cyfrowa stanowi jeden z czynników wyboru i współpracy z bankiem, co z kolei stymuluje innowacyjność instytucji finansowych, tym bardziej, że banki odczuwają konkurencję ze strony fintechów (Klimontowicz 2019, s. 89–97).

Występuje również podejście wskazujące, że istota banku cyfrowego związana jest z doświadczeniem klienta (ang. *customer experience*)[1], gdzie oferuje się kontekstualne, mobilne usługi, które zmieniają tzw. podróż klienta (ang. *customer journey*)[2]. Bycie bankiem cyfrowym oznacza dostarczanie atrakcyjnych i istotnych doświadczeń, dzięki wykorzystaniu otwartej, zintegrowanej i elastycznej architektury technologicznej. Ilustruje to równanie wyrażające jakościową sumę trzech cech banku cyfrowego (D) (*Digital Banking* 2017, s. 5):

[1] Jest to efekt interakcji między bankiem a klientem w dłuższym czasie, sprowadzający się do wykorzystania zdobytej wiedzy analitycznej dla osiągnięcia licznych korzyści zarówno dla banku, jak i dla klientów.

[2] Podróż klienta opisuje różne formy kontaktu potencjalnego i faktycznego klienta z produktem lub marką – od pierwszego postrzegania aż do momentu podjęcia decyzji o zawarciu transakcji i staniu się lojalnym klientem.

$$D = A + B + C,$$

gdzie:

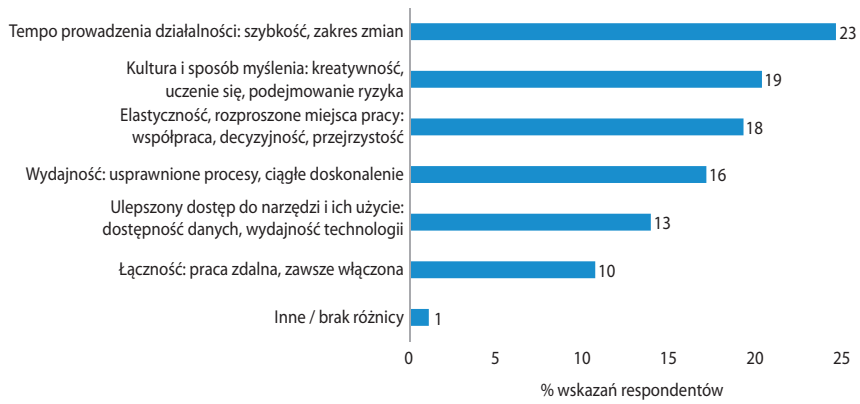
A = **zawsze i wszędzie, każdy kanał** – dostarcza tego, czego oczekują klienci, niezależnie od tego, czy są to masowi klienci banku detalicznego, czy klienci segmentu *private banking* – czyli inwestorzy o wysokiej wartości netto (ang. *high net worth individual* – HNWI), czy korporacje; wszystkie te oczekiwania prowadzą do tego, że bank musi dostosowywać się do tych wymogów; tym samym eliminowane są ograniczenia czasowe i przestrzenne.

B = **lepsza bankowość** – poza świadczeniem tradycyjnych usług bankowych wykorzystuje się koncepcję doradcy wirtualnego, pomagającego klientowi w podejmowaniu decyzji finansowych.

C = **kontekstowy** – bank oferuje usługi (produkty), komunikację (formy obsługi) tak dopasowane, aby sprostać indywidualnym oczekiwaniom klientów dotyczącym personalizacji na podstawie zaawansowanych analiz informacji i danych o kliencie oraz zdiagnozowanych lub prognozowanych potrzeb.

Ponadto bank cyfrowy odznacza się tym, że bazą jego poznawania klienta są informacje i dane o kliencie oraz otoczeniu, ich analiza z wykorzystaniem zaawansowanej aparatury statystycznej czy ekonometrycznej oraz technologii cyfrowych. Rezultaty tych procesów wpływają na kształtowanie modeli biznesowych, wybór celów opracowywanie strategii i priorytety inwestycyjne, podejście do wdrażania innowacji, strukturę organizacyjną, kulturę organizacyjną/kulturę ryzyka, system wartości, stosowane narzędzia – czyli kluczowe elementy zarządzania bankiem. W istocie cyfrowość prowadzi do procesów zmian systemu zarządzania ryzykiem w bankach.

Rysunek 1. Największe różnice pomiędzy działalnością w środowisku cyfrowym i tradycyjnym



Źródło: Kane, Phillips, Copulsky i Andrus 2019.

Warto podkreślić, że istnieją zasadnicze różnice pomiędzy bankami cyfrowymi i bankami zarządzanymi tradycyjnie (rys. 1). Dotyczą one m.in. roli technologii, innowacyjności, kultury i rodzajów kluczowych wskaźników efektywności. Przeprowadzono liczne badania dotyczące różnic kulturowych pomiędzy organizacjami tradycyjnymi a tymi nastawionymi na innowacje technologiczne. Z tych badań wynika, że banki cechują się zwłaszcza czterema wartościami związanymi z kulturą cyfrową: **wpływem**, **szybkością**, **otwartością** i **autonomią** (ang. *impact*, *speed*, *openness*, *autonomy*) (tabela 1). Dodatkowo, niespotykane wcześniej tempo wdrażania sztucznej inteligencji wskazuje, że istotnym zagadnieniem staje się w erze cyfrowej konieczność dodatkowego uwzględnienia wartości etycznych. Do nich przykładowo zalicza się (McDonald 2015, s. 73):

- uczciwość i rzetelną informację,
- szacunek dla ochrony prywatności,
- szacunek dla respektowana praw własności, zwłaszcza oprogramowania,
- unikanie powodowania strat/kosztów/zakłóceń sprzecznych z działaniami łączącymi się z cyberbezpieczeństwem,
- szacunek dla ochrony środowiska.

Tabela 1. Cztery kluczowe wartości kultury cyfrowej

Wpływ	Szybkość	Otwartość	Autonomia
Radykalne zmienianie świata poprzez permanentne innowacje.	Szybkie, iteracyjne kroki – jako przeciwieństwo czekania na zebranie wszystkich odpowiedzi przed podjęciem działania.	Szerokie zaangażowanie, zbieranie danych, materiałów z różnorodnych źródeł, dzielenie się radami i informacjami w sposób otwarty, zamiast zachowywania wiedzy dla siebie.	Pozwolenie ludziom na wysoki poziom zaufania i delegowania zadań, aby robili to, co należy zrobić, zamiast polegania na formalnie zorganizowanym zarządzaniu i wyznaczonych politykach.

Źródło: Westerman, Soule i Eswaran 2019.

Na tle tych rozważań o bankowości cyfrowej warto podjąć próbę oceny aktualnego stanu zarządzania ryzykiem w bankach w Polsce, które dokonały już w różnym stopniu dostosowań do działania w środowisku cyfrowym. Podstawą do tej oceny będą wyniki badania empirycznego wybranej grupy respondentów z banków liczącej 127 osób.

2. Wyniki badania empirycznego dotyczącego systemu zarządzania ryzykiem w bankach[3]

W badaniu skoncentrowano się na ocenie aktualnego systemu zarządzania ryzykiem w bankach w warunkach rozwoju cyfryzacji. Przesłanki podjęcia analiz w tym obszarze wynikają m.in. z (na podstawie: Węgrzyn i Zaczek 2023, s. 31–44; Szpringer 2023, s. 95–111; Kasiewicz i Kurkliński 2022, s. 31–45; Kruk i Gąsiorkiewicz 2022 s. 81–97; Szaniewski 2022, s. 114–126; Poniatowska-Jaksch 2021, s. 15–32; Rostek 2021, s. 80–101; Głogowski 2021, s. 238–252):

1) Potrzeby włączenia w system zarządzania organizacjami (w tym w szczególności bankami) zaawansowanych i złożonych mechanizmów zapewniania bezpieczeństwa procesów podstawowych.
2) Konieczności konkurowania przez banki z innymi podmiotami świadczącymi usługi finansowe.
3) Dużej niestabilności uwarunkowań regulacyjnych, społeczno-kulturowych, politycznych, gospodarczych itd.
4) Systematycznie nasilających się procesów cyfryzacji życia, w tym także procesów społeczno-gospodarczych, a także rosnących wymagań społeczeństwa względem cyfryzacji procesów (m.in. związanych ze świadczeniem usług finansowych).
5) Dostępności coraz bardziej zaawansowanych i jednocześnie bezpiecznych technologii teleinformatycznych.

W badaniu zastosowano podejście indukcyjne, gdzie na podstawie analizy jednostkowych obserwacji podjęto próbę generalizacji empirycznej analizowanych zjawisk i szacowanych zależności (Sułkowski 2012, s. 95 i nast.; Dobrzycka 2014, s. 281 i nast.; Wojciechowska 2016, s. 116 i nast.). Wykorzystano także elementy podejścia dedukcyjnego, głównie na etapie krytycznej analizy krajowych i zagranicznych źródeł literaturowych. W ramach podejścia indukcyjnego zastosowano następujące ilościowe empiryczne techniki badawcze (na podstawie: Sudoł 2012, s. 136–145; Apanowicz 2005, s. 57 i nast.; Zaborek 2009, s. 41–49; Turek 2010, s. 161 i nast.; Wojciechowska 2011, s. 47–54): technikę badania ankietowego CAWI (ang. *Computer-Assisted Web Interview*) oraz technikę statystycznej analizy danych ilościowych. Badanie zostało przeprowadzone w okresie marzec–kwiecień 2023 roku przy wsparciu – na etapie zbierania danych – Instytutu Badawczego IPC Sp. z o.o. z siedzibą we Wrocławiu. W kwestionariuszu ankiety znalazły się pytania z wariantami odpowiedzi, które respondenci wartościowali w zaproponowanej skali opisowej.

Oryginalna próba badawcza liczyła 232 osoby, a respondenci byli przypisani do czterech grup, tj.: (1) banków – 54,74%, (2) fintechów – 25,86%, (3) firm technologicznych (IT) – 8,62%, a także (4) środowiska akademickiego – 10,78%. Podstawą kwalifikowania respondentów do danej grupy było realizowanie przez nich działań powiązanych z zarządzaniem ryzykiem, procesami innowacyjnymi lub projektami

[3] Szersze *spectrum* wyników zostało zawarte w publikacji: Woźniak 2024, s. 99 i nast.

rozwojowymi, albo zaangażowanie w te procesy jako podmioty zewnętrzne. **Natomiast w niniejszym artykule wykorzystano wyłącznie odpowiedzi respondentów zaliczonych do segmentu banki** (tabela 2).

Tabela 2. Rodzaje banków, w których zatrudnieni byli respondenci (N=127)

Rodzaj banku	%
Reprezentuję duży bank uniwersalny	38,58
Reprezentuję średni bank	29,92
Reprezentuję bank z dominującym kapitałem polskim	8,66
Reprezentuję bank spółdzielczy	8,66
Reprezentuję oddział instytucji kredytowej (bank zagraniczny)	6,30
Reprezentuję bank specjalistyczny	5,51
Reprezentuję bank zrzeszający BS-y	1,58
Reprezentuję bank z dominującym kapitałem zagranicznym	0,79
Razem	**100,00**

Źródło: opracowanie własne.

Zasadniczym celem badania było poznanie opinii respondentów, jak banki w Polsce podchodzą do kształtowania systemu zarządzania ryzykiem w warunkach cyfryzacji procesów w perspektywie 2035 roku. Respondentów pytano:

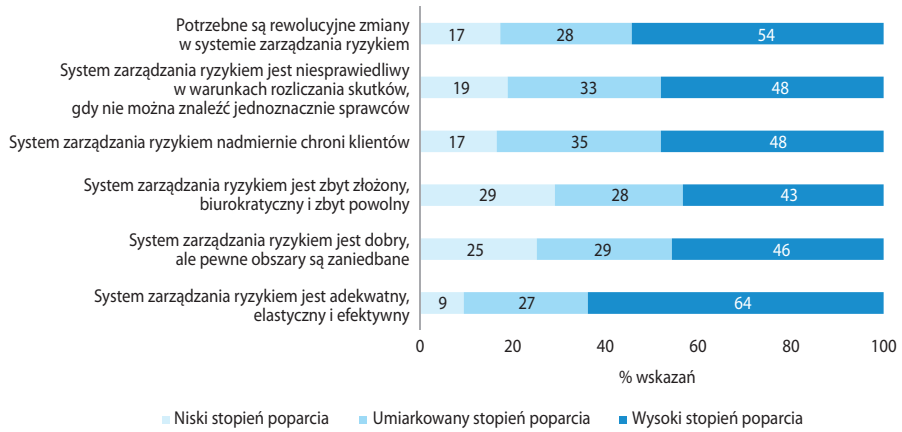
1) Jakie jest podejście banków w Polsce do kształtowania swojego rozwoju w zakresie zarządzania ryzykiem?
2) Jakie są uwarunkowania i jakie jest zaawansowanie transformacji cyfrowej banków w Polsce?
3) Jakie są podstawowe efekty transformacji cyfrowej banków w Polsce – w kontekście zarządzania ryzykiem?

Przedmiotem eksploracji była hipoteza: Banki zdążą zmodernizować system zarządzania ryzykiem do stanu jego rozwoju w perspektywie roku 2035.

2.1. Podejście banków do kształtowania swojego rozwoju w zakresie zarządzania ryzykiem

Podstawą rozważań o perspektywie 2035 r. była diagnoza aktualnego stanu systemu zarządzania ryzykiem (rys. 2).

Rysunek 2. Struktura ocen respondentów w zakresie aktualnego stanu systemu zarządzania ryzykiem w sektorze bankowym (N=127)

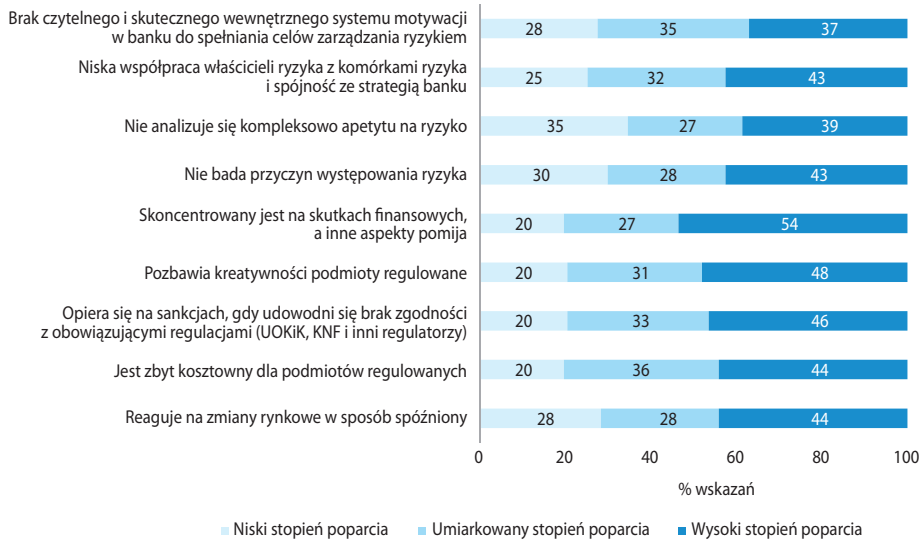


Źródło: opracowanie własne.

Analizując wyniki przedstawione na rysunku 2, można dostrzec niespójność opinii respondentów. Pierwsze trzy cechy aktualnego systemu zarządzania ryzykiem potwierdzają, że respondenci są świadomi, jak poważną rolę odgrywa zarządzanie ryzykiem w funkcjonowaniu banków. Jest to pozytywna ocena dotychczasowej pracy banków i instytucji regulacyjno-nadzorczych. Dostrzegają oni też pewne obszary zaniedbań – zgodnie z tym, że nic nie jest doskonałe. Jednak trudno pominąć fakt, że nowe rodzaje ryzyk, a także potencjalne możliwości, jakie wiążą się z wykorzystaniem sztucznej inteligencji, wskazują, iż potrzeba bardziej przełomowych zmian w systemie zarządzania ryzykiem. Ta cecha nie dotyczy aktualnego systemu zarządzania, ale jest klarownym wyzwaniem dla podjęcia działań w bliższej lub dalszej przyszłości. Ponadto istotną informacją są te opinie, które znalazły się na najdalszych pozycjach, bo one odzwierciedlają nierozwiązane problemy. Powinny być przedmiotem szczególnego zainteresowania, aby dążyć do ich usprawnienia. Warto podkreślić, że te oceny aktualnego stanu systemu zarządzania ryzykiem w dużym stopniu odnoszą się do „tradycyjnego" modelu zarządzania ryzykiem i oznaczają, iż nie oczekuje się, aby system zarządzania ryzykiem miał podlegać zasadniczej zmianie. Może to świadczyć o braku świadomości pilności koniecznych zmian w paradygmacie zarządzania ryzykiem w bankach i ich otoczeniu regulacyjnym.

Najważniejsze słabości aktualnego systemu zarządzania ryzykiem w sektorze bankowym w opinii respondentów przedstawiono na rysunku 3.

Rysunek 3. Struktura ocen respondentów w zakresie słabości aktualnego systemu zarządzania ryzykiem w sektorze bankowym (N=127)

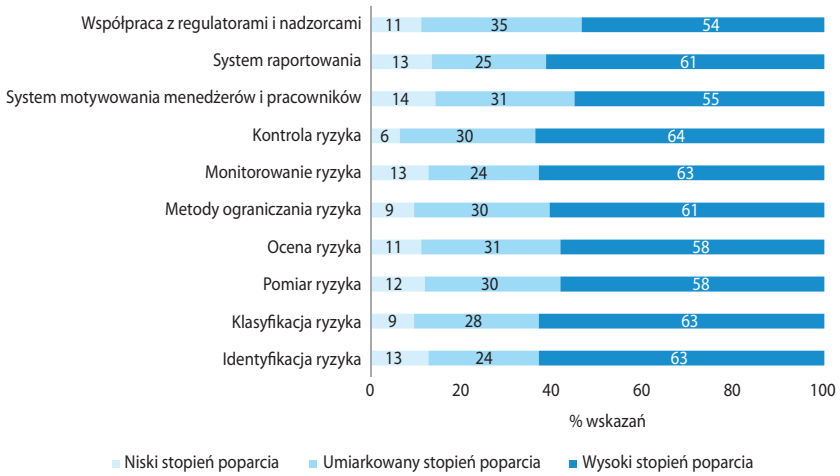


Źródło: opracowanie własne.

Analizując rysunek 3, można zauważyć, że niedoceniany jest problem radykalnej zmiany podejścia regulatorów do systemu wdrażania regulacji, aby nadawać większą rangę narzędziom stymulującym pożądane zachowania banków, a nie ograniczać się do nakładania coraz wyższych kar. Ponadto, za zbyt optymistyczne uznać można powszechne przyjmowanie założenia o w miarę prostym i bezproblemowym uwzględnieniu w praktyce kryteriów o charakterze niefinansowym (np. celów ESG). Dopóki nie zostaną skorygowane zakorzenione przyzwyczajenia i przepisy prawne dotyczące egoistycznie komercyjnych motywacji właścicieli banków, to pożądane cele środowiskowe, społeczne i zarządcze mogą pozostać w zbyt dużej części w sferze dobrych praktyk, czego przejawem mogą być niektóre działania anty ESG w ustawodawstwie niektórych stanów w USA (por. Krosinsky 2023, s. 69–70).

Ocenę jakości głównych etapów zarządzania ryzykiem w bankach w opiniach respondentów zaprezentowano na rysunku 4.

Rysunek 4. Struktura ocen respondentów w zakresie jakości głównych etapów zarządzania ryzykiem w bankach (N=127)



Źródło: opracowanie własne.

Analizując rysunek 4, można zauważyć, że respondenci oceniają umiarkowanie pozytywnie dwa bloki działań typowych dla zarządzania ryzykiem. Pierwszy łączy się z monitorowaniem, kontrolą, klasyfikacją i identyfikacją ryzyka. Drugi blok obejmuje system motywowania, współpracę z regulatorami, pomiar i ocenę ryzyka. Wyżej oceniane są etapy zarządzania zaliczane do pierwszej grupy. Niepokojące jest to, że najsłabiej wypada działający w bankach system motywowania pracowników i menedżerów, skłaniający ich do koncentracji na obniżaniu skutków negatywnych związanych z ryzykiem. Ten wynik skłania to zastanowienia się, jakie są istotne przyczyny takiej sytuacji. Wydaje się, że może to wynikać ze słabości planowania kluczowych wskaźników efektywności, z niedostatecznej alokacji odpowiedzialności osób za uzyskiwane rezultaty, wysokiej automatyzacji procesów związanych z ryzykiem, czy niskiej szkodliwości występujących ryzyk. Nie można też wykluczyć, że podział obowiązków w obszarze zarządzania ryzykiem w bankach między komórki i pracowników nie jest dostatecznie transparentny. Ponadto banki powinny w większym stopniu, niż jest to obecnie praktykowane, zachęcać pracowników do poszukiwania nowych instrumentów i narzędzi eliminacji lub ograniczania ryzyka, np. poprzez dokonywanie eksperymentów i wymianę informacji o sprawdzonych dobrych praktykach.

2.2. Uwarunkowania i zaawansowanie transformacji cyfrowej banków

Z przeprowadzonego badania wynika, że generalnie banki nie odczuwają silnych barier w transformacji cyfrowej, co jest dość wyjątkowym zjawiskiem w funkcjonowaniu instytucji finansowych. Niepokoi jednak niska ocena dla poziomu zarzą-

dzania kulturą ryzyka, gdyż jest to uznana determinanta cyfrowego sukcesu rynkowego banków. Zagadkowy jest też rezultat badania dotyczący niskiego poziomu informatyzacji banków, gdy uznaje się, że banki pod względem dostosowania się do zmian charakterystycznych dla ery cyfrowej są lokowane w czołówce nie tylko krajowej, ale i europejskiej. Wydaje się, że taka opinia spowodowana jest nadal wysokim udziałem wykorzystywania informacji w formie papierowej.

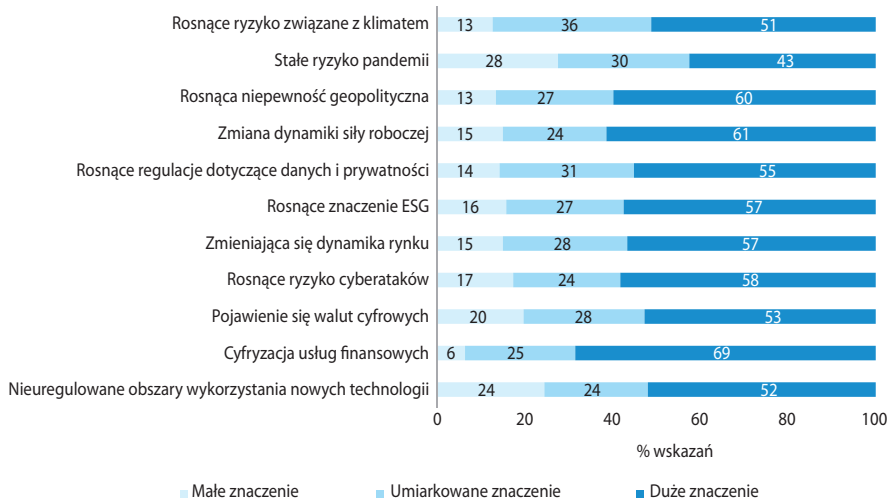
Respondenci eksponowali także potrzebę zacieśnienia współpracy i partnerstwa regulatorów z interesariuszami. Relacje te powinny być rozwijane od momentu określenia wstępnych celów i założeń opracowanego projektu regulacyjnego, a nie koncentrować się na egzekucji, gdy regulacje są już wprowadzone dyrektywami, ustawami, rozporządzeniami czy choćby rekomendacjami. Spornymi kwestiami w tych relacjach są: racjonalny podział ryzyka między „graczy" rynkowych, zachowanie zasady proporcjonalności i dążenie do rozwoju rynku usług bankowych bez konieczności nakładania wysokich barier i nadmiernych obciążeń. Ilustruje to np. rozporządzenie w sprawie wyposażania bankomatów w system barwiący banknoty, które weszło w życie 23 września 2023 roku, aby ograniczyć napady na bankomaty. Kłopot będą mieli operatorzy bankomatów, bo koszty wprowadzenia tego zabezpieczenia są zbyt dotkliwe, np. dla części banków spółdzielczych. Nadto przewidziano zbyt krótki okres *vacatio legis* (3 miesiące) na dostosowanie się banków do przepisów tego rozporządzania[4]. Z kolei wydaje się, że coraz szersza potrzeba rozwiązywania problemów o charakterze kulturowym lub etycznym będzie sprzyjała pogłębieniu współpracy między regulatorami a bankami.

Koncentrując uwagę na szansach dla banków w najbliższej dekadzie, jako źródłach ich długofalowego rozwoju, warto zauważyć, że respondenci dość trafnie identyfikują przyszłe kierunki zmian – o ile władze banków będą wspierać i aktywnie działać w tych obszarach. Warto podkreślić, że banki niewystarczająco doceniają obszar ryzyka ewentualnych pandemii czy katastroficznych zdarzeń w następstwie zmian klimatu, niepokojów społecznych lub pożądanych standardów władztwa korporacyjnego (rys. 5).

Kolejnym zagadnieniem odnoszącym się do uwarunkowań rozwoju banków jest znaczenie celów banków w perspektywie najbliższej dekady (rys. 6).

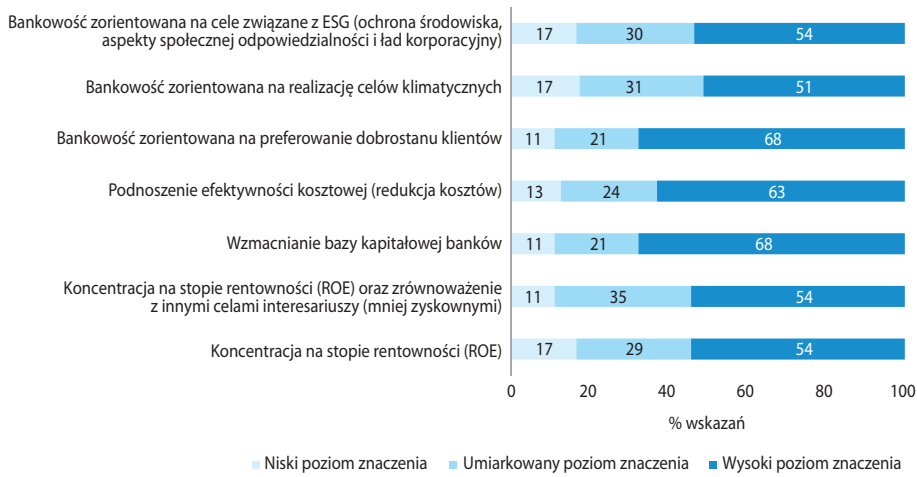
[4] MSWiA zaproponowało przedłużenie *vacatio legis* rozporządzenia w sprawie systemów barwiących. MSWiA proponuje, aby termin został przedłużony do 1 stycznia 2024 r. Zob. BS NET z dn. 11 września 2023 r.

Rysunek 5. Struktura ocen respondentów w zakresie szans dla banków w najbliższej dekadzie (N=127)



Źródło: opracowanie własne.

Rysunek 6. Struktura ocen respondentów w zakresie celów banków w perspektywie najbliższej dekady (N=127)



Źródło: opracowanie własne.

Analizując rysunek 6, można zauważyć, że najwyższy poziom realizacji celów banków w perspektywie najbliższej dekady respondenci identyfikują z celami „tradycyjnymi", co można interpretować w ten sposób, że banki nie będą skłonne do

frontalnego przejścia do podjęcia się myślenia i działania zgodnego z ewolucją zarządzania ryzykiem. Warto podkreślić, że w procesie transformacji cyfrowej priorytetowe cele są całkowicie odmienne. W szczególności dotyczy to: równoważenia osiągania efektów finansowych z dążeniem do realizacji planów w obszarze ESG, nowego modelu konkurowania, czy kolejności podejmowanych trafnych działań w obszarze wdrażania technologii teleinformatycznych.

Zagłębiając się w problematykę uwarunkowań rozwoju i transformacji cyfrowej banków w Polsce, warto zwrócić uwagę na główne strategie banków dla utrzymania konkurencyjności (rys. 7).

Rysunek 7. Struktura ocen respondentów w zakresie głównych strategii banków dla utrzymania konkurencyjności (N=127)

Źródło: opracowanie własne.

Według respondentów banki w głównej mierze ukierunkowują swoje strategie na konkurencję w cyberprzestrzeni, koncentrując się m.in. na obszarze płatności, przeciwdziałaniu praniu brudnych pieniędzy, ochronie przed oszustwami/wyłudzeniami i inwestowaniu w ochronę danych. Interesujące jest również to, że banki cenią sobie działania w zakresie poprawy doświadczeń klientów (rys. 7). Zatem, strategie banków z jednej strony dotyczą cyfryzacji, a z drugiej – wartości postrzeganych i wymaganych przez klientów. Uwidacznia się więc znowu swoista „polaryzacja" działań banków – z jednej strony myślenie o „nowoczesności", a z drugiej strony „zakorzenienie w tradycyjnym podejściu", co w zasadniczy sposób może hamować zmianę podejścia do zarządzania ryzykiem.

Kolejnym ważnym zagadnieniem z punktu widzenia poruszanej w artykule problematyki jest struktura odpowiedzi respondentów odnośnie do głównych kierunków transformacji cyfrowej w bankach (rys. 8).

Rysunek 8. Struktura ocen respondentów w zakresie zaawansowania transformacji cyfrowej w bankach – kierunki działań (N=127)

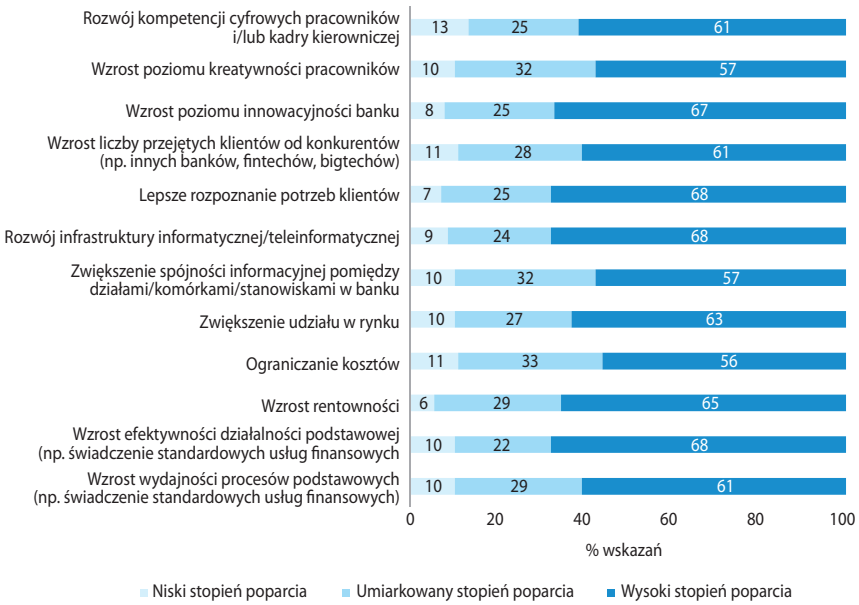
Źródło: opracowanie własne.

Analiza rysunku 8 wskazuje, że banki w zakresie transformacji cyfrowej działają wieloaspektowo. Jednakże uwidacznia się m.in. to, że koncentrują się przede wszystkim na automatyzacji wielu procesów podstawowych, jak również zaawansowanej analityce danych oraz wykorzystaniu mediów cyfrowych. Pokazuje to ewidentne ukierunkowanie banków na podejście nowoczesne, które w pewnym sensie wymusza, a w zasadzie powinno wymuszać, zupełnie inne podejście do zarządzania ryzykiem, np. w aspekcie ryzyka rynkowego lub operacyjnego, czy też ryzyka związanego z cyberzagrożeniami. Z drugiej strony transformacja cyfrowa to dla banków również konieczność inwestowania w infrastrukturę informatyczną, co wydaje się być mało efektywne. Zdarzają się już bowiem w bankach przykłady przejścia na technologie „chmurowe", tj. związane m.in. z utrzymywaniem danych klientów na zewnętrznych serwerach. Oczywiście, korzystanie z outsourcingu IT pociąga za sobą konieczność zmian w zakresie stosowanych metod i procedur zarządzania ryzykiem, ale jednocześnie może być postrzegane jako swoisty „kamień milowy" w transformacji cyfrowej.

2.3. Podstawowe efekty transformacji cyfrowej banków – w kontekście zarządzania ryzykiem

Przedstawiona ocena uwarunkowań i zaawansowania transformacji cyfrowej banków w Polsce może posłużyć jako przesłanka dla identyfikacji podstawowych efektów związanych z jednej strony z implementacją określonych technologii teleinformatycznych, a z drugiej powiązania tych efektów z możliwościami zmiany paradygmatu zarządzania ryzykiem.

Rysunek 9. Struktura ocen respondentów w zakresie efektów transformacji cyfrowej w bankach (N=127)



Źródło: opracowanie własne.

Z analizy rysunku 9 wynika, że do głównych efektów transformacji cyfrowej banków należą: rozwój infrastruktury informatycznej/teleinformatycznej, lepsze rozpoznanie potrzeb klientów, a także wzrost efektywności działalności podstawowej (np. świadczenie standardowych usług finansowych). Z kolei względnie najsłabszymi efektami są: zwiększenie spójności informacyjnej pomiędzy działami/komórkami/stanowiskami w banku, wzrost poziomu kreatywności pracowników oraz wzrost liczby przejętych klientów od konkurentów (np. innych banków, fintechów, bigtechów) i rozwój kompetencji cyfrowych pracowników i/lub kadry kierowniczej. Taki stan rzeczy wskazuje, że w bankach mogą potencjalnie zaistnieć istotne „kulturowe" ograniczenia w zmianie paradygmatu zarządzania ryzykiem. Wynika to z tego, że swoistą podstawą ewolucji podejścia do postrzegania ryzyka oraz zarządzania nim są działania pracowników i kadry kierowniczej. Jeśli transformacja cyfrowa nie wywiera silnego efektu na modyfikację działań ludzi, to z dużym prawdopodobieństwem nie zmieni się ich podejście w obszarze zarządzania ryzykiem. Warto tu odwołać się chociażby do kreatywności pracowników – kreatywność, jako efekt transformacji cyfrowej, nie odnosi się wyłącznie do pojawiania się nowych usług finansowych w bankach. Dotyczy także systematycznego rozwijania mechanizmów zarządzania w banku.

Podsumowanie

Można zaryzykować stwierdzenie, że **zarządzanie ryzykiem w sektorze bankowym w Polsce znajduje się na rozdrożu**. Z jednej strony okazało się, że banki wdrożyły obowiązujący system zarządzania ryzykiem. Jest on nadal zakorzeniony w tradycyjnej działalności banków, mimo znaczącego postępu w transformacji cyfrowej. Z drugiej strony ujawniły się słabości cyfryzacji działalności banków w obszarach kultury cyfrowej, w tym wartości cyfrowych, stosowania wielkich baz danych, zaawansowanej analityki, generatywnej sztucznej inteligencji, ochrony prywatności, a także w walce z przestępstwami cyfrowymi. **W tym aspekcie ukształtowanie i sukcesywna implementacja nowego paradygmatu zarządzania ryzykiem wydaje się wymogiem przyszłości**, w szczególności jeśli chodzi o respektowanie takich zasad, jak: koncentruj się na tych rodzajach ryzyka, które przyniosą ci największe korzyści, maksymalizuj „efektywność ryzyka", bądź profesjonalnie przygotowany na nowe najbardziej nieoczekiwane ryzyka, a także dokonaj głębokiej decentralizacji zarządzania ryzykiem.

Bibliografia

Apanowicz J. (2005), *Metodologiczne uwarunkowania pracy naukowej*, Difin, Warszawa.

Barquin S., Vinayak H.V. (2016), *Building a digital-banking business*, McKinsey & Company.

Digital Banking (2017), Temenos Headquarters S.A.

Dobrzycka M. (2014), *Strategie badawcze stosowane w naukach ekonomicznych*, [w:] K. Kuciński (red.), *Naukowe badanie zjawisk gospodarczych. Perspektywa metodologiczna*, Wolters Kluwer, Warszawa.

Ginovsky J. (2015), *What really is digital banking?*, „Banking Exchange", 01.04.2015.

Głogowski A. (2021), *Wymiary ryzyka systemowego w finansach cyfrowych*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Informatyzacja, cyfryzacja i danetyzacja*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Kane G.C., Phillips A.N., Copulsky J., Andrus G. (2019), *How Digital Leadership Is(n't) Different*, „MIT Sloan Management Review", Spring.

Kasiewicz S., Kurkliński L. (2022), *Bankowość internetowa i mobilna*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Perspektywa rynkowa*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Kelman J. (2016), *The History of Banking: A Comprehensive Reference Source & Guide*, Create Space Independent Publishing Platform.

Klimontowicz M. (2019), *Innowacyjność banków komercyjnych w Polsce – ujęcie modelowe*, Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach, Katowice.

Krosinsky C. (2023), *Zrównoważone inwestowanie w USA*, „Bezpieczny Bank", tom 93, nr 4.

Kruk M., Gąsiorkiewicz L. (2022), *Internet rzeczy w działalności ubezpieczeniowej*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Perspektywa rynkowa*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

McDonald G. (2015), *Business Ethics a Contemporary Approach*, Cambridge University Press.

Poniatowska-Jaksch M. (2021), *Gospodarka cyfrowa i jej miary*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Informatyzacja, cyfryzacja i danetyzacja*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Rostek K. (2021), *Technologie cyfrowe*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Informatyzacja, cyfryzacja i danetyzacja*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Sudoł S. (2012), *Nauki o zarządzaniu. Podstawowe problemy i kontrowersje*, Polskie Wydawnictwo Ekonomiczne, Warszawa.

Sułkowski Ł. (2012), *Epistemologia i metodologia zarządzania*, Polskie Wydawnictwo Ekonomiczne, Warszawa.

Szaniewski D. (2022), *Big Data Analytics w ubezpieczeniach*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Perspektywa rynkowa*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Szpringer W. (2023), *Systemy płatności w epoce cyfrowej*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Nowe tendencje i możliwości*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Turek D. (2010), *Mierzalność zjawisk w naukach ekonomicznych*, [w:] K. Kuciński (red.), *Metodologia nauk ekonomicznych. Dylematy i wyzwania*, Difin, Warszawa.

Westerman G., Soule D.L., Eswaran A. (2019), *Building Digital-Ready Culture in Traditional Organizations*, "MIT Sloan Management Review", Summer.

Węgrzyn J., Zaczek A. (2023), *Cyfryzacja sektora finansów publicznych*, [w:] L. Gąsiorkiewicz, J. Monkiewicz (red.), *Finanse cyfrowe. Nowe tendencje i możliwości*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Wojciechowska R. (2011), *Proces badawczy w naukach ekonomicznych*, Szkoła Główna Handlowa w Warszawie, Warszawa.

Wojciechowska R. (2016), *Logika procesu badawczego w ekonomii*, Szkoła Główna Handlowa w Warszawie, Warszawa.

Woźniak J. (2024), *Cyfryzacja banków w warunkach zarządzania ryzykiem*, [w:] S. Kasiewicz, J. Woźniak, *Podróż banków do nowego modelu zarządzania ryzykiem. Perspektywa 2035 roku*, Warszawski Instytut Bankowości, Warszawa.

Zaborek P. (2009), *Qualitative and quantitative research methods in management science*, [w:] M. Strzyżewska (red.), *Selected methodological issues for doctoral students*, Warsaw School of Economics, Warsaw.

Recenzje

DOI: 10.26354/bb.8.1.94.2024

Jan Szambelańczyk*
ORCID: 0000-0002-4340-5193
Jan.Szambelanczyk@poznan.merito.pl

Recenzja książki Krzysztofa Kalickiego, Michała Jabłońskiego, *Rynek walutowy. Odesłania do tabel kursowych*, Wydawnictwo Naukowe SCHOLAR, Warszawa 2024, s.166

Rynek walutowy to immanentna składowa bankowości i finansów o wyraźnej specyfice merytorycznej i o tym traktuje recenzowana książka. Brak kompetencji w przeprowadzaniu transakcji walutowych może prowadzić do poważnych konsekwencji dla podmiotów tego rynku, zarówno w skali makro-, mikro- czy osób fizycznych. Aby wyeksponować, o jakie konsekwencje chodzi, na tle sporu kredytobiorców z bankami, można zestawić łączne szacunkowe koszty niekorzystnych dla instytucji kredytowych wyroków na kwotę przekraczającą 200 mld zł oraz wartość środków z Krajowego Programu Odbudowy[1]. Porównanie to uzmysławia finansową skalę problemu, a kontrowersje można określić mianem debaty narodowej.

Ze względu na cechy istoty funkcjonowania systemu ekonomicznego w Polsce, przed transformacją z lat 90., nieliczni rezydenci mieli wiedzę na temat 'sekretów' rynku walutowego. Od tamtych czasów poziom zaawansowania technologii i technik funk-

* Jan Szambelańczyk – profesor zwyczajny w Uniwersytecie WSB Merito w Poznaniu.

1 Według założeń z KPO Polska otrzyma 59,8 mld euro, z tego 25,27 mld euro w postaci dotacji i 34,54 mld euro w formie preferencyjnych pożyczek. Kwota ewentualnych kosztów dla banków w przypadku spełnienia tzw. czarnego scenariusza jest niewiele mniejsza wartości KPO i niemal dwukrotnie większa niż wartość dotacji z tego Programu.

cjonowania tego rynku czy asortyment oferowanych usług finansowych uległy bardzo dużym zmianom. Nadto, ewentualne doświadczenia z 'cinkciarstwa' w okresie PRL, z jakim miało do czynienia stosunkowo wielu mieszkańców naszego kraju, to jedynie przedszkolne przygotowanie do sprawnego poruszania się po współczesnym rynku walutowym. W ówczesnych warunkach niedostępność kredytu w walutach wymienialnych dla rezydentów krajowych nie kształtowała ani indywidualnych kompetencji, ani społecznej świadomości ryzyka związanego z tego typu transakcjami. Używając kategorii 'kompetencje', mam na myśli nie tylko wiedzę, umiejętności i ewentualnie doświadczenie klienta, ale także cechy osobowości człowieka[2], z którymi wiąże się jego postawa, w tym skłonność do podejmowania ryzyka. Można postawić hipotezę, że dotyczyło to także poważnej części kadry instytucji finansowych.

Na przełomie tysiącleci formułowano optymistyczne projekcje szybkiego rozwoju Polski. Takie były również dominujące nadzieje czy oczekiwania społeczne. Obejmowały one m.in. spodziewane przystąpienie do strefy euro. Ponadto istotny wpływ na zachowania klientów i instytucji finansowych miał ówcześnie korzystny kurs polskiej waluty (PLN), szczególnie w stosunku do franka szwajcarskiego (CHF), tym bardziej, że koszty kredytów w walucie krajowej były wyraźnie wyższe w porównaniu do kredytów w głównych walutach światowych. Szeroki kontekst sytuacyjny, a zwłaszcza wskazane w poprzednich zdaniach uwarunkowania, motywowały znaczną część klientów instytucji finansowych w Polsce do wyboru kredytów walutowych, a ściślej kredytów denominowanych czy indeksowanych do walut obcych. W takich warunkach, bez dodatkowych ograniczeń – ze strony banku czy regulatora dotyczących ryzyka kursowego, zdolność kredytowa klientów była wyższa dla kredytów nominowanych czy indeksowanych do walut obcych, szczególnie zaś do franka szwajcarskiego. Wszystko to na rynku kredytów mieszkaniowych doprowadziło do wyraźnej polaryzacji kredytobiorców (złotowi vs walutowi). Nie można zapominać, że podobne zachowania dotyczyły podmiotów gospodarczych, zatrudniających profesjonalne kadry finansowe, czego przykładem były straty jakie na opcjach walutowych czy transakcjach terminowych poniosły nawet przedsiębiorstwa zaliczone do kategorii kluczowych. Do dziś trudno o wiarygodną diagnozę przyczyn polaryzacji postaw klientów, którzy decydowali się na kredyty złotowe lub walutowe tym bardziej, że przez wiele lat okazywało się, że oczekiwania kredytobiorców walutowych – co do niższych stóp oprocentowania oraz niższych łącznych kosztów kredytów – sprawdzały się. Sytuacja uległa zmianie dopiero wtedy gdy wystąpiły trudno przewidywalne wydarzenia na rynku globalnym. Były to m.in. słabość dolara, czy euro oraz zmiany w polityce Banku Centralnego Szwajcarii wraz z proinflacyjną polityką NBP, które wywołały głęboką deprecjację kursu złotego. Trudno o jednoznaczną diagnozę korzyści lub strat spolaryzowanych segmentów kredytobiorców, w których były subsegmenty czy też niehomogeniczne grupy klientów, z punktu widzenia sytuacji finansowej, a zwłaszcza życiowej w powiązaniu z kredytowanym mieszkaniem czy mieszkaniami.

[2] Kategoria kompetencji zasadniczo wyparła w nowoczesnej praktyce HR (ang. Human Resources) kwalifikacje, co związane jest z postępem nauk społecznych, które dostarczają instrumentów przydatnych w zarządzaniu, zwanych niekiedy miękkimi kwalifikacjami.

Brak kompetencji czy choćby ugruntowanych doświadczeń kredytobiorców na rynku finansowym i w zarządzaniu ryzykiem prowadził do kultywowania narodowej przywary zwerbalizowanej już przez Mikołaja Reja („*Polak nie mądr, aż po szkodzie*") czy Jana Kochanowskiego („*Nową przypowieść Polak sobie kupi, że i przed szkodą i po szkodzie…*"). Tym bardziej, że konflikty kredytobiorców walutowych i banków miały już miejsce od lat 70. XX w. w Australii czy, nieco później, w niektórych krajach europejskich. Niestety, na tle tych zagranicznych doświadczeń zabrakło przysłowiowej mądrości instytucjonalnej, edukacji finansowej społeczeństwa czy adekwatnego mitygowania ryzyka. Zamiast tego kierowano się krótkookresowymi korzyściami, lekceważono zasadę zdroworozsądkowej przezorności, o bardziej zaawansowanych sposobach kształtowania zachowań czy zarządzania ryzykiem nie wspominając[3]. Niestety, po stronie rządzącej klasy politycznej i decydentów także zabrakło odpowiednich działań we właściwym czasie.

W konsekwencji zarysowanych procesów i zachowań podmiotów rynku finansowego w Polsce od niemal dwóch dekad w narodowej debacie o problemie kredytów mieszkaniowych/hipotecznych indeksowanych kursem lub denominowanych w walucie obcej uczestniczą zarówno najważniejsze gremia decyzyjne w kraju; od prezydenta, rządu, KSF, NBP, KNF, UOKiK czy polityków począwszy po banki, prawników, publicystów i wreszcie rzesze kredytobiorców oraz ich powinowatych albo utworzonych stowarzyszeń pokrzywdzonych przez system bankowy. Ostry, a nadto silnie „podgrzewany" przez interesariuszy zewnętrznych (pierwotnie głównie kredytobiorców i polityków, a później na skutek ewidentnych interesów finansowych kancelarii prawnych) konflikt znajduje wielotysięczne finały w sądach krajowych[4], a nawet w TSUE. Gdyby pominąć imponderabilia toczonych na wielu płaszczyznach i forach sporów, główną jego oś stanowiłby dylemat prymatu norm prawnych vs rudymentarnych praw ekonomii i finansów[5]. Takie ujęcie istoty sporu w kontekście umów cywilno-prawnych klientów i banków prowadzi do wniosku, że osiągnięcie konsensusu w warunkach przyjmowania różnych aksjomatów stron, jakie wyznają antagoniści, jest niemożliwe[6]. W bardziej wysublimowanej formie można dopatrywać się kardynalnej zmiany interpretacji prawnej umów kredytowych w Polsce,

[3] Ówcześnie symptomatyczna dla postaw znacznej części społeczeństwa była maksyma: „maksymalizacji korzyści własnych, przy upublicznianiu nakładów buforowana nacjonalizacją strat", która jak wykazuje praktyka nie straciła na aktualności.

[4] W tym aspekcie trudno pominąć powstanie superlukratywnej niszy rynkowej dla środowiska prawniczego o wartości przychodów szacowanych przynajmniej na dziesiątki miliardów złotych. W kręgach wtajemniczonych w transakcje P&A na rynku kancelarii prawnych w Polsce mówi się o „niebotycznych" stopach zwrotu z takich transakcji, w oczekiwaniu na korzyści z masowych wyroków sądów w sporach tzw. frankowiczów z bankami.

[5] Ewidentnym tego przykładem są interpretacje przepisów, a także orzeczenia sądów, w konsekwencji których wartość pieniądza w czasie ma zerową wartość.

[6] *Tout proportion gardée*, gdyby wskazany dylemat sprowadzić do konfliktu aksjomatów, wówczas nasuwa się analogia do dylematu głównej bohaterki słynnej antycznej tragedii autorstwa Sofoklesa „Antygona". Chodzi o to, że tytułowa antyczna postać musi wybrać pomiędzy posłuszeństwem władcy (władzy ludzkiej, politycznej), a posłuszeństwem prawom boskim. Przypominam, że decydując się na to drugie, Antygona swój wybór okupiła śmiercią, gdyż za nieposłuszeństwo władcy została skazana na śmierć głodową, a zamurowana w piwnicy – powiesiła się.

w szczególności na drodze radykalnych odwołań do przepisów konsumenckich UE, które zresztą powstawały wcześniej niż zasadniczy wolumen kredytów walutowych w naszym kraju.

Nakreślony wyżej kontekst systemowy stanowi ważne tło dla tematyki książki i rozważań autorstwa Krzysztofa Kalickiego i Michała Jabłońskiego. Publikacja traktuje nie tylko o zawiłościach funkcjonowania rynków walutowych, ale formułuje także silnie uargumentowane wątpliwości: „co do poprawności i uzasadnienia prawnego wielu wyroków w sprawach kredytów walutowych, szczególnie w ostatnich latach"(s.12). Już ta syntetyczna informacja kształtuje potencjalne grono zainteresowanych recenzowanym opracowaniem. Wykorzystując funkcję recenzenta na pierwszym miejscu w gronie interesariuszy, podobnie zresztą jak autorzy, wskażę środowisko prawników reprezentujących kredytobiorców, bądź banki, ale również sędziów, którym przychodzi rozstrzygać złożone merytorycznie i formalnie spory finansowe. A przecież istota tych sporów należy merytorycznie do różnych dyscyplin w naukach społecznych, ze szczególnym uwzględnieniem ekonomii i finansów oraz nauk prawnych. W dalszej kolejności można by rozważać kontekst behawioralny zachowań stron sporu, z odpowiednim uwzględnieniem finansów behawioralnych i psychologii społecznej. Jak się wydaje ten aspekt problematyki kredytów frankowych pozostaje jeszcze do zagospodarowania choć szkoda, że nie są dostępne reprezentatywne badania i wyniki w tym obszarze.

Wskazując potencjalnych interesariuszy ustaleń autorów, nie można pominąć reprezentantów ogniw sieci bezpieczeństwa finansowego oraz akademików w roli badaczy lub nauczycieli. Wreszcie, do zapoznania się z opracowaniem K. Kalickiego i M. Jabłońskiego warto zachęcić dziennikarzy i publicystów, których działalność istotnie wpływa na kształtowanie opinii publicznej.

W teorii kardynalna dla prawomocności ustaleń jest moc poznawcza argumentu, bądź wyjaśnienia. Jednak w rozważaniach i analizach problematyki podejmowanej w recenzowanej książce nie bez znaczenia jest także to, kto odpowiednie argumenty lub wyjaśnienia i na jakiej podstawie formułuje. Zresztą bezpośrednio dotyczy to sformułowanego powyżej dylematu priorytetu ekonomii i finansów vs nauk prawnych[7]. Mam tu m.in. na uwadze konieczną koordynację złożonych merytorycznie i interdyscyplinarnych problemów praktycznych. Z tego punktu widzenia autorzy książki mają bardzo dobre rekomendacje. Krzysztof Kalicki jest dr. hab. nauk ekonomicznych, pracującym na stanowisku profesora w Akademii Leona Koźmińskiego w Warszawie o bogatej karierze zawodowej w finansach i bankowości, w tym na wysokich stanowiskach decyzyjnych w sektorze publicznym i prywatnym[8]. Michał Jabłoński jest dr. nauk prawnych i wykładowcą w Zakładzie Ekonomicznej Anali-

[7] Mark Blaug, znany brytyjski ekonomista, we wprowadzeniu do swej bestselerowej książki „Economics of education"(1970) napisał: „jak ktoś coś umie robić to to robi, jak nie umie robić uczy, jak nie umie ani robić, ani uczyć prowadzi badania, a najgorsi są ci co piszą książki", dodając, że ma nadzieję iż sam nie podpada pod tą regułę. W tym samym duchu przywołuję kompetencje autorów recenzowanej książki.

[8] Szerzej Krzysztof Kalicki – Wikipedia, wolna encyklopedia

zy Prawa Uniwersytetu Warszawskiego, specjalizującym się w prawie publicznym, procedurach stanowienia prawa, z bogatą praktyką adwokacką w sądach krajowych oraz TSUE[9].

W ukierunkowaniu percepcji wywodu autorów ważne miejsce zajmuje bardzo przystępnie napisane 'Wprowadzenie', zawierające zarys historii kredytów frankowych w Polsce. Pozwala ono czytelnikowi, w przysłowiowej pigułce, przypomnieć sobie lub poznać genezę i istotę sporu stron umów kredytowych, a w pewnym stopniu także roli otoczenia regulacyjnego i politycznego w tej kwestii. Dość nietypowo, jak na tradycję pisarską, zaraz po 'Wprowadzeniu' autorzy zamieszczają „Zasadnicze tezy opracowania" (1,5 strony tekstu), które z racji usytuowania w książce 'bez dowodu' pozwalają zorientować się w dominującym nurcie narracji i wnioskach autorskich. Natomiast właściwe dowody znajdujemy w dalszej części książki. Przyjęte przez Autorów rozwiązanie można potraktować jako chęć zainteresowania i zmotywowania czytelnika do poszukiwania odpowiednich uzasadnień tych tez w części I lub części II książki.

Poza tymi dwoma fragmentami wstępnymi książka składa się z dwóch wyraźnie ze sobą powiązanych problemowo części: pierwszej zatytułowanej „Specyfika rynku walutowego i rzeczywistości gospodarczej w wyrokach dotyczących spraw kredytów walutowych" i drugiej pt. „Wymóg sprecyzowania metodologii ustalania kursu waluty obcej w umowie kredytu denominowanego lub indeksowanego w świetle wykładni prawa unijnego w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej oraz polskich sądów". Szkoda, że nie postarano się o prostsze zredagowanie tych tytułów (np. specyfika rynku walutowego na tle praktyki ekonomicznej i judykatury; wymóg formuły kursu walutowego w umowie kredytu denominowanego lub indeksowanego w walucie obcej).

Część I książki podzielona jest na 15 rozdziałów traktujących m.in. o szczegółowych zagadnieniach funkcjonowania rynku walutowego, specyfice i zasadach, skali i strukturze operacji oraz mechanizmach działania rynków walutowych, kursach walut, arbitrażu walutowym, segmentach rynku walutowego, rynku kasowym, platformach transakcyjnych i informacyjnych, różnicach kursów średnich NBP i kursów rynkowych, tabelach kursowych, spread'ach, wreszcie o wymianie walut w kontekście postanowień umów kredytowych. Kolejne rozdziały pozwalają zorientować się lub zrozumieć złożoność i meandry procesów oraz transakcji na rynku walutowym. Zawierają one schematy i tabele liczbowe ilustrujące omawiane procesy w ujęciach dynamicznych. Za ułatwiające zrozumienie rozważań czy wręcz instrukcyjne uznać można większość eksponowanych w specjalnych ramkach wniosków K. Kalickiego. Przy czym wnioski te mają różną naturę poznawczą, od eksperckich generalizacji po dyrektywy praktyczne. Jednocześnie ułatwiają czytelnikowi syntetyczne ujęcie fragmentów rozważań w poszczególnych rozdziałach.

[9] Szerzej Centrum Oceny Skutków Regulacji (uw.edu.pl).

Poniżej charakteryzuję dziesięć wybranych wniosków z części I.

Wniosek (s. 29): *konkurencja na rynku detalicznym wraz z nowoczesnymi technologiami i elektronicznymi kanałami komunikacji sprawiają,* że rynkowe kursy dla klienta detalicznego są transparentne i efektywne, a *spread'y rynkowe (różnice między ceną kupna i sprzedaży plus marża agenta) sukcesywnie zmniejszają się, tym bardziej, że klienci-nabywcy mogą swobodnie wybierać oferenta potrzebnej waluty.*

Wniosek (s. 31 i 37): *wolny i wysoce konkurencyjny rynek uniemożliwia dowolność w ustalaniu oferowanych kursów walut w relacji do rynku, bez ponoszenia negatywnych skutków finansowych takiej dowolności. Dzieje się tak bowiem arbitraż walutowy w segmencie hurtowym, jak i detalicznym nie pozwala na istotne odchylenia od kursu rynkowego.*

Wniosek (s. 41): *nie ma* żadnej *niezawodnej metody ustalania jednolitego kursu dla dowolnej pary walutowej na całym rynku. Dotyczy to także prognozowania kursów, których poprawność zależy od systemu założeń (zbioru czynników i ich parametrów) przyjmowanych przez dany podmiot, w tym subiektywnych przewidywań odnośnie do przyszłości.*

Wniosek (s. 68 i 69): *już w latach 90. platformy tradingowe działające w czasie rzeczywistym zapewniały wysoki poziom transparencji kursów walut na rynku hurtowym, a ewentualne odchylenia od tych notowań były nieistotnie małe albo wręcz marginalne. Natomiast przynajmniej od 2000 r. nie było lepszych niż rynkowe notowania kursów na platformach tradingowych, co dodatkowo czyniło je wysoce transparentnymi.*

Wniosek (s. 72): s*pecyfika rynku walutowego, jego decentralizacja, wielość źródeł informacji, techniczne warunki błyskawicznego porównania konkurencyjności ofert wreszcie możliwość stosowania arbitrażu walutowego systemowo wymuszają dostosowywanie oferowanych kursów do warunków rynkowych z ewentualnymi marginalnymi odchyleniami. Głównie dlatego formułowany niekiedy postulat punktowego odtworzenia kursu przez klienta jest ze względów techniczno-organizacyjnych, a przede wszystkim konieczności poniesienia niezbędnych kosztów praktycznie niewykonalny.*

Wniosek (s. 84): *klienci/konsumenci praktycznie nie mają dostępu do systemów transakcyjnych ani nie posiadają know-how posługiwania się tymi systemami, co czyni niewykonalnym weryfikowanie przez nich są kursów transakcyjnych banku zmieniających się w sposób ciągły*.

Wniosek (s. 99 – pierwsze zadanie): *spread'y walutowe, czyli różnice pomiędzy ceną kupna i sprzedaży danej waluty plus wynagrodzenie dla podmiotu zajmującego się wymianą walutową, zależą od wielu czynników, ponadto na rynkach hurtowych są zmienne z częstotliwością milisekund, podobnie jak kursy walut, które je determinują.*

Wniosek (s. 103): *często uzasadnienia wyroków sporządzane przez sędziego w kwestii dowolności banku co do ustalania kursów albo spread'ów*, bądź *marż nie odpowiadają rzeczywistym procesom, zwłaszcza zaś możliwości istotnego ich odbiegania*

od poziomów rynkowych. Dowodzą tego m.in. kwotowania banków, kantorów i fintechów, które różnią się tylko o dziesiętne lub setne części grosza, co przesądza o tym, że obiektywnym kursem referencyjnym jest kurs rynkowy.

W zależności od stopnia znajomości problematyki mniejsze lub większe trudności w przyswojeniu przekazu Autora – w użytej stylizacji językowej – mogą nastręczać przynajmniej trzy wnioski.

Wniosek (s. 20): „*Rynki walutowe są dostępne dla instytucji i osób fizycznych w sposób ciągły. Brak regulacji, wysoka płynność i swoboda transakcji implikują wysoką efektywność rynku i jego transparencję. W świecie rynków elektronicznych zajęcie pozycji w walucie oznacza ryzyko dla obu stron transakcji – traderzy i ich partnerzy handlowi zwykle zajmują pozycję w określonej walucie – kupując lub sprzedając po najkorzystniejszej akceptowanej dla obu stron cenie. Otwarcie pozycji ryzyka wynika z interesu ekonomicznego partnerów.*

Wniosek (s. 88): „*Oczekiwanie, że bank ustali idealnie działający algorytm tworzenia kursu średniego do zbudowania tabeli jest teoretycznie i praktycznie niewykonalne, o ile bank nie będzie brał na siebie ryzyka zmienności i płynności rynku w czasie i ryzyka rozbieżności kursów między wybranymi platformami a innymi platformami istniejącymi na rynku*".

Wniosek (s. 99 – drugie zadanie): „*[…] Spready hurtowe przenoszą się na spready detaliczne i korygowane są o podobne źródła kosztów specyficzne dla detalu, w tym również ryzyko mrożenia kursów kupna i sprzedaży oferowanych klientom w tabelach w ciągu dnia*".

Część I książki kończy oryginalne podsumowanie autorskie (s. 112–116) napisane nie tylko ze znawstwem merytorycznym problematyki rynku walutowego, ale także silnym ładunkiem emocjonalnym osoby mającej bogate doświadczenia osobiste w monitorowaniu i nadzorze nad procesami i transakcjami walutowymi. K. Kalicki eksponuje specyfikę rynku walutowego – jako rynku nieregulowanego, działającego 24 godziny na dobę przez 5 dni w tygodniu, wykorzystującego wysoce zaawansowane technologie informatyczne na globalnym rynku, do ultraszybkiego i zautomatyzowanego wyznaczania transparentnej ceny danej waluty. Dodatkowo akcentuje, że rynek walutowy nie jest jednolity czy homogeniczny, ale składa się z różnych segmentów wyróżnionych z punktu widzenia uczestniczących w nim podmiotów lub rodzajów technologii – zwłaszcza platform jedno- i wielo-dostępnych, umożliwiających globalną konkurencję w sposób ciągły dzięki stosowanym algorytmom dla określonego wolumenu obrotu. Wszystko to sprawia, że nie da się ustalić jednego uniwersalnego kursu średniego dla całego rynku, ani jednego algorytmu kalkulacji. Tym bardziej, że każdy bank opracowuje i stosuje własną metodę pobierania próbek informacji i kalkulacji stosowanej średniej stawki na rynku. Również rynek hurtowy będący podstawowym źródłem informacji o kursach walut obejmuje różnego rodzaju platformy – informacyjne i transakcyjne – co wpływa na różnice w pojawiających się notowaniach. Systemy transakcyjne dotyczą także różnych segmentów – transakcji międzybankowych i brokerskich, instytucji dealerskich, dealerów

detalicznych itp. Oznacza to, że dostęp do rzeczywistych kwotowań zmieniających się w milisekundach nie jest taki sam dla wszystkich uczestników globalnego rynku. Dlatego też postulat udostępniania wzorów matematycznych czy algorytmów pozwalających na weryfikację bankowych kursów walut przez konsumentów jest nierealistyczny i nie ma racji bytu w praktyce, a może mieć – co najwyżej – charakter teoretycznej abstrakcji (o kosztach takich działań, nie wspominając)[10]. W tych okolicznościach konkurencyjny rynek w mechanizmie popytu, podaży i arbitrażu walutowego stanowi najlepszą i najbardziej przejrzystą weryfikację konkurencyjności banków.

Ze scharakteryzowanych procedur oraz analiz empirycznych wynika, że dynamiczne zmiany kursów walut, a także zmiany kosztów, w tym regulacyjnych i ryzyka, implikują poziom spread'ów walutowych, które dodatkowo zmieniają się w zależności od rodzaju waluty, wolumenu transakcji, czasu trwania oferty (od milisekund do dziennych tabel stawek kursowych), itp. Nieznajomość tych specyficznych i wysoce złożonych mechanizmów rynku walutowego przyczynia się do formułowania wadliwych ocen zachowań banków, nieuzasadnionych zarzutów o nadużycia pozycji profesjonalisty w stosunku do nieprofesjonalnego klienta, formułowania wobec banków nierealistycznych żądań, wreszcie stymulowanie antybankowych postaw społecznych, a nawet orzeczeń sądowych opartych na takich fałszywych opiniach albo nierealistycznych przesłankach.

Część II książki ustrukturyzowano w dziewięć fragmentów traktujących głównie o recepcji tez Wyroku TSUE przez polskie sądy, odwołaniach do tabel kursowych banków w orzecznictwie sądów w okresie poprzedzającym Wyrok TSUE, znaczeniu odesłania prejudycjalnego i roli TSUE, wymogu przejrzystości warunku umownego w kontekście klauzuli ryzyka kursowego, analizie Wyroku TSUE w kontekście treści pytań prejudycjalnych, skutkach braku przejrzystości warunku umownego, rekonstrukcji rozstrzygnięcia zawartego w Wyroku TSUE.

Część II kończy syntetyczne podsumowanie (s. 148–150), w którym M. Jabłoński uwzględnia zarówno ustalenia analizy ekonomicznej K. Kalickiego, jak i własne wyniki analiz prawnych. Odsyłając czytelników do odpowiednich partii tekstu, warto wyeksponować następujące ustalenia:

- osiągnięcie wskazanego w Wyroku TSUE stopnia przejrzystości klauzul przeliczeniowych w praktyce jest niewykonalne, zwłaszcza w kwestii umożliwienia konsumentowi w dowolnym momencie samodzielnego ustalenia kursu wymiany stosowanego przez bank (przedsiębiorcę),
- w świetle art. 5 Dyrektywy 93/13 przejrzystość klauzuli umownej jest stopniowalna, a skomplikowanie formuły kalkulacyjnej nie przesądza jeszcze o abuzywności, zresztą podobnie wypowiadał się w tej kwestii w swych wyrokach TSUE, natomiast orzecznictwo polskich sądów „powierzchownie implementuje wytyczne TSUE",

[10] *Nota bene* można także wskazać, że na wolnym rynku nikt nie kontroluje merytorycznie tabel kursowych banków centralnych.

- warunek umowy niespełniający wymogu przejrzystości może być uczciwy, jeżeli odpowiada wymogowi dobrej wiary i nie wprowadza znaczącej nierównowagi stron, ze szkodą dla konsumenta, co w świetle Wyroku TSUE pozostaje do szczegółowej oceny sądu krajowego,
- w orzecznictwie sądów w Polsce najczęściej stosuje się ewidentnie uproszczone, a nawet nieuprawnione w świetle Wyroku TSUE, przeniesienie oceny o nieprzejrzystości postanowień umownych na tezę o przyznaniu sobie przez bank uprawnienia do arbitralnego kształtowania kursu wymiany,
- możliwe jest uznanie, że kurs wskazany w tabeli kursowej banku ma charakter rynkowy, a postanowienie umowne odsyłające do tej tabeli nie wprowadza znaczącej nierównowagi praw i obowiązków ze szkodą dla konsumenta, tym bardziej, że ustawa antyspredowa została uchwalona dopiero w 2011 r., a znaczna część umów kredytów ma datę wcześniejszą,
- ze względu na postanowienia art.1 ust.2 Dyrektywy Rady 93/13 (co pominął w swych orzeczeniach TSUE) oraz treści umów kredytu denominowanego i indeksowanego, w których nie określono zasad ustalania kursów walut, zawartych przed wejściem w życie ustawy antyspreadowej odpowiadają obowiązującemu ówcześnie stanowi prawnemu.

Autorzy wykazują 122 pozycje literatury i źródeł wykorzystanych w pracy, w tym 67 opracowań zagranicznych, w których znajdujemy pozycje klasyków ekonomii i finansów (np. B. Balassa czy P.A. Samuelsona), Encyklikę Fratelli Tutti Ojca Świętego Franciszka o braterstwie i przyjaźni społecznej z 2020 r., opracowania międzynarodowych i krajowych instytucji finansowych (np. FED, BIS, NBP, KNF), publikacje prestiżowych instytucji analityczno-badawczych (np. IIE, NBER), witryny globalnych platform medialnych (np. Bloomberg, Thomson Reuters) i inne. Tekst uzupełniają instrukcyjne schematy, tabele i rysunki ilustrujące zmiany na rynkach walutowych wybranych krajów, głównie w latach 1992–2010 oraz według wybranych transakcji spot. W Aneksie zamieszczono cztery tabele oraz syntezę 10 wyroków polskiego Sądu Najwyższego z okresu poprzedzającego wyrok TSUE. W doborze kierowano się przede wszystkim kwestią łączenia abuzywności klauzul przeliczeniowych z odesłaniem do tabel kursowych banków (s. 163–166). Zebranie tych orzeczeń w Aneksie istotnie ułatwia zrozumienie wywodów Autora w zasadniczej treści II części książki.

Połączenie kompetencji merytorycznych autorów wzbogacone rozległymi doświadczeniami praktycznymi, dostępem do informacji insider'skiej, skoordynowaną współpracą ekonomisty – praktyka bankowego i prawnika – czynnego adwokata, *last but not least* osobistym zaangażowaniem w problematykę podejmowaną w książce, sprawiają, że powstało unikalne i wysoce użyteczne opracowanie, które pozytywnie wyróżnia się w dostępnym piśmiennictwie, a także debacie o kredytach walutowych. Sformułowane oceny i wnioski mogą mieć także niebagatelne znaczenie dla rozstrzygania sporów klientów i banków w kwestii kredytów frankowych. Szczególnie wobec ryzyka podważania elementarnych praw ekonomii i finansów, a zwłaszcza kanonu wartości pieniądza w czasie.

Uważam, że nie wszystkie fragmenty książki i sformułowane konkluzje są łatwe w odbiorze pozwalającym na operacyjne zrozumienie. Przyczyną tego jest przede wszystkim złożoność i specyfika materii, szczególnie dla czytelników nieznających codzienności procesów, procedur i transakcji na rynku walutowym albo nie obytych z rozległymi, rozproszonymi, a nadto nie zawsze jednoznacznymi regulacjami prawnymi. Z drugiej zaś strony niekiedy redakcja tekstu nie ułatwia szybkiego czytania lub przyswojenia przesłania autorów (dwa przykłady zawarto we wcześniejszej partii tej recenzji). Może to więc niekiedy ograniczać samodzielne stosowanie ustaleń w praktyce.

Niezależnie od tych ułomności znaczenie problematyki podejmowanej w książce oraz zapotrzebowanie praktyki społecznej zdecydowanie przemawiają za zapoznaniem się z rozważaniami, analizami i wnioskami autorów.

Uwzględniając aktualność problematyki kredytów walutowych oraz masową skalę interesariuszy rozwiązania sporów z nimi związanych, z pozycji recenzenta rekomenduję przygotowanie II wydania książki, przede wszystkim w wersji elektronicznej, po uprzedniej starannej weryfikacji redakcji tekstu, z ukierunkowaniem na uproszczenie lub objaśnienie wysoce specjalistycznych zagadnień lub sformułowań. Mam tu na względzie, że nie wszyscy czytelnicy mają specjalistyczne przygotowanie do odbioru i zrozumienia zaawansowanych merytorycznie, technicznie czy technologicznie zjawisk lub procesów, o których mowa w książce.

Zachęcam także autorów do refleksji nad zasadnością usytuowania R-11 i R-12 w obecnej sekwencji rozdziałów części I. Podobnie jeżeli chodzi o kolejność R-2, R-3, R-4 i R-5 w części II.

Sądzę, że wprowadzenie sugerowanych korekt redakcyjnych i ewentualnie zmian kolejności rozdziałów spowoduje, że recenzowana publikacja stanie się kanonem literaturowym nie tylko dla praktyków prawa, ale będzie wykorzystywana na wykładach monograficznych dla studentów i doktorantów czy na studiach podyplomowych.

Lektura książki K. Kalickiego i M. Jabłońskiego, a zwłaszcza zawarte w niej informacje, analizy i wnioski przekonują, że warto rekomendować ją wszystkim interesariuszom rynku walutowego, a dla uczestników sporów w kwestii kredytów walutowych można jej nadać kolokwialną etykietę *must read*.

W marcu 2024 r.