RYNEK FINANSOWY

AUTORZY:

Grzegorz BLICHARZ
Bartłomiej ORĘZIAK
Emil RATOWSKI
Kamil RATOWSKI
Patryk WALCZAK
Marcin WIELEC

RYNEK FINANSOWY

Zapobieganie przyczynom przestępczości

Redakcja: Grzegorz Blicharz, Bartłomiej Oręziak, Marcin Wielec

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI | **Warszawa 2021**

MINISTERSTWO
SPRAWIEDLIWOŚCI
www.ms.gov.pl

FUNDUSZ
SPRAWIEDLIWOŚCI

Współfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

RECENZENCI *dr hab. Norbert Malec, prof. UPH w Siedlcach*
dr hab. Piotr Krzysztof Sowiński, prof. UR

OPRACOWANIE REDAKCYJNE *Teresa Naumiuk*
PROJEKT OKŁADKI, SKŁAD, ŁAMANIE *Bogusław Słomka*

WYDANIE 2

ISBN 978-83-66344-89-1

WYDAWNICTWO INSTYTUTU WYMIARU SPRAWIEDLIWOŚCI
ul. Krakowskie Przedmieście 25, 00-071 Warszawa
SEKRETARIAT tel.: (22) 630-94-53, fax: (22) 630-99-24, e-mail: wydawnictwo@iws.gov.pl

DRUK, OPRAWA *„Elpil", ul. Artyleryjska 11, 08-110 Siedlce*

Spis treści

Wstęp

Niniejsze opracowanie stanowi produkt prac analitycznych podejmowanych przez Zespół Implementacyjny w ramach projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" organizowanego przez Instytut Wymiaru Sprawiedliwości, w obszarze rynku finansowego. W opracowaniu, co oczywiste, przedstawiono jedynie wybrane zagadnienia, związane z tytułowym problemem. Składają się nań teksty autorstwa sześciu ekspertów. Monografia naukowa dotyczy istotnych oraz aktualnych zagadnień związanych z przeciwdziałaniem przestępczości finansowej oraz metodami zapobiegania jej przyczynom. Sektor finansowy stanowi jeden z najważniejszych filarów polskiej gospodarki, który wpływa na prawidłowe oraz bezpieczne funkcjonowanie państwa. Z tego powodu przedmiotowa problematyka zasługuje na szczególną uwagę praktyki, teorii oraz legislatury. Efektywne eliminowanie przestępczości na rynku finansowym wymaga sformułowania konkretnych metod zwalczania tego rodzaju aktywności, a w szczególności wskazania odpowiednich działań zapobiegawczych. Zaproponowane w niniejszym opracowaniu rozwiązania stanowią istotne głosy w dyskusji na temat przemian, jakim ulegać powinno polskie prawo, oraz na jakie zagadnienia powinni zwrócić uwagę prawodawcy w aspekcie zwiększania bezpieczeństwa sektora finansowego.

Celem niniejszego opracowania jest omówienie procesu podejmowania decyzji w instytucjach finansowych. Przeprowadzona analiza uregulowań dotyczących wskazanego zagadnienia pozwoli uwypuklić ryzyka oraz rodzaje przestępczej działalności, z którymi muszą się mierzyć podmioty działające na rynku finansowym. Umożliwi także sformułowanie propozycji *de lege ferenda*, mających ograniczyć ryzyko przestępczości związane z działalnością

instytucji finansowych. Na wstępie należy także wskazać, że omawiane procesy muszą być zawsze dostosowane do środowiska, w jakim działają instytucje finansowe, tj. do systemu finansowego. Istotnym punktem odniesienia dla prowadzonych analiz stały się porządki zarówno innych państw Europy, jak i Stanów Zjednoczonych, Chin czy Australii, gdzie prawodawcy stykają się z wyzwaniami dynamicznie rozwijających się rynków finansowych. Dialog między porządkami *common law* i *civil law* w przypadku regulacji na rynku finansowym wskazuje, że istnieje płaszczyzna porównawcza, która także ma swoje źródła w europejskiej tradycji prawnej oraz racjonalności i użyteczności ekonomicznej wpisanej w naturę prawa[1].

Pierwszy rozdział zawiera wprowadzenie do tematyki rynku finansowego oraz jego modeli. W jego ramach omówiono rolę systemu finansowego w gospodarce, modele systemu finansowego, funkcje systemu finansowego, rodzaje rynku finansowego i jego uczestników, instytucje finansowe, instytucje bankowe i ich operacje oraz instytucje regulujące i nadzorujące.

Drugi rozdział podejmuje problem rozwiązań organizacyjnych ułatwiających zachowanie kontroli instytucji finansowej nad operacjami realizowanymi przez jej pracowników. W jego ramach omówiono zmianę charakteru prawnego rekomendacji Komisji Nadzoru Finansowego oraz ich wpływu na reguły postępowania z dobrem i bezprawność czynu, konstruowanie szczególnej komórki ds. odpowiedzialności podmiotów zbiorowych (*Criminal Compliance*), regulację pozycji prawnej sygnalistów, program sygnalistów na przykładzie rozwiązań prawa amerykańskiego w perspektywie prawa polskiego oraz propozycję nowelizacji art. 304 Kodeksu karnego.

Trzeci rozdział dotyczy analizy procesu podejmowania decyzji w instytucjach finansowych. W jego ramach omówiono różne modele podejmowania decyzji oraz zaproponowano postulaty *de lege ferenda*. Kluczowym momentem przedmiotowego rozdziału jest badanie komparatystyczne dotyczące systemów prawnych Niemiec, Szwajcarii oraz Włoch.

Czwarty rozdział to analiza zarządzania operacjami w instytucjach finansowych. W jego ramach omówiono modele zarządzania w instytucji finansowej oraz przedstawiono postulaty *de lege ferenda*, w ramach których

[1] F. Longchamps de Bérier, *Finansowa analiza prawa a znaczenie prawa rzymskiego*, „Forum Prawnicze" 2013, nr 5(19), s. 14–16.

znajdują się propozycje dotyczące rejestru transakcji walut wirtualnych oraz wprowadzenia jednolitej licencji bankowej.

Piąty rozdział odnosi się do zarządzania ryzykiem w instytucjach finansowych. W jego ramach omówiono źródła ryzyka, analizy i zarządzanie ryzykiem, ryzyko związane z prowadzeniem działalności gospodarczej, sposoby reagowania na ryzyko, ryzyko w działalności instytucji finansowych oraz ryzyko przestępczości finansowej.

Szósty rozdział obejmuje analizę przygotowania obrony przed różnymi formami ataków na instytucje finansowe. W jego ramach omówiono problematykę cyberprzestępczości oraz dokonano badania komparatystycznego dotyczącego typów nowoczesnych przestępstw w systemach prawnych Niemiec, Włoch, Chin oraz Australii.

Siódmy rozdział dotyczy analizy działalności międzynarodowych grup przestępczych oraz metod zapobiegania im w instytucjach finansowych. W jego ramach omówiono umowy międzynarodowe i akty unijne regulujące zagadnienie przestępczości międzynarodowej w związku z instytucjami finansowymi, polskie regulacje odnoszące się do przedmiotowych przestępstw oraz charakterystykę przestępstw o charakterze międzynarodowym w instytucjach finansowych popełnianych przez grupy przestępcze.

Ósmy rozdział dotyczy analizy i metod zapobiegania przestępstwom finansowym dokonywanym przez klientów instytucji finansowych. W jego ramach omówiono przestępczość na rynku bankowym, przestępczość na rynku ubezpieczeń, przestępczość na rynku kapitałowym, pranie pieniędzy z przestępstw oraz zarządzanie bezpieczeństwem instytucji finansowych.

Dziewiąty rozdział został poświęcony zaprezentowaniu założeń projektowych oraz analizie *de lege lata* typów czynów zabronionych w obszarze finansowym w Polsce. W związku z powyższym, w pierwszej kolejności przedstawiono płaszczyznę badawczą, wytyczne dotyczące podejmowanych prac oraz metodologię. Następnie przybliżono konkretne czyny zabronione związane z szeroko rozumianym rynkiem finansowym w polskim systemie prawnym: Kodeks karny skarbowy, Kodeks karny oraz Kodeks spółek handlowych. Przedmiotowy rozdział zawiera także pozostałe typy czynów zabronionych (pozakodeksowe typy czynów zabronionych) oraz katalog najważniejszych aktów prawnych na rynku finansowym.

Monografia naukowa kończy się zwięzłym sprawozdaniem z warsztatu naukowego dotyczącego zagadnienia przeciwdziałania przyczynom przestępczości na rynku finansowym, który został zorganizowany 25 marca 2019 roku w siedzibie Instytutu Wymiaru Sprawiedliwości.

Redaktorzy

ROZDZIAŁ PIERWSZY

Rynek finansowy i jego modele

Przeciwdziałanie przestępczości w sferze rynku finansowego może odbywać się na wielu poziomach. Jednym z nich jest dbanie o kulturę organizacyjną, a zatem o sprawne zarządzanie organizacjami finansowymi, które pozwoli z jednej strony na rozwijanie postaw praworządnych, a z drugiej – na zmniejszenie ryzyka występowania przestępczości w samych organizacjach. Zagadnienie skutecznego przeciwdziałania przestępczości zależy naturalnie nie tylko od właściwej kultury organizacyjnej czy sposobów zarządzania pracownikami, lecz także od aspektów technologicznych. W tym wymiarze kluczowe znaczenie odgrywa troska o cyberbezpieczeństwo, dbanie o właściwe zarządzanie operacjami finansowymi, a także o opracowanie strategii biznesowych, które uwzględniają innowacyjne sposoby walki z przestępczością w sektorze finansowym.

1.1. Rola systemu finansowego w gospodarce

System finansowy stanowi jeden z podstawowych elementów współczesnej gospodarki. Od stanu systemu finansowego, jego zorganizowania i skuteczności procedur w dużym stopniu zależy przebieg procesów ekonomicznych w krajowej gospodarce. Nieprawidłowości w funkcjonowaniu systemu finansowego, występujące między innymi w formie kryzysów finansowych, skutkują dostrzegalnym wzrostem zainteresowania regułami działania systemu finansowego. Kryzys finansowy bywa zwykle impulsem do zmian w systemie finansowym. Jako przykład posłużyć mogą inicjatywy wprowadzane w życie po kryzysie z 2008 r. Jasnym wydaje się, że propozycje zmian

w funkcjonowaniu systemu finansowego muszą być poprzedzone dyskusją z szerokim udziałem środowisk eksperckich. Za przykłady takiego działania uznać można analizy Larosiere[2], Liikanena[3], Vickersa[4] czy Volckera[5]. Stanowiły one opracowanie dotychczasowych problemów systemu rynków finansowych oraz były impulsem wypracowania zmian w systemach finansowych krajów Unii Europejskiej, a także Stanów Zjednoczonych. W raporcie Komisji Europejskiej, poświęconym sektorowi finansowemu, wskazano, że: *Celem nadrzędnym programu reform finansowych UE jest stworzenie systemu finansowego, który służy gospodarce i umożliwia zrównoważony wzrost gospodarczy*[6]. Stwierdzenie to wskazuje na pożądane kierunki reformy finansowej. Zgodnie z nim system finansowy powinien pełnić pomocniczą rolę w gospodarce oraz wspierać wzrost gospodarczy, w przeciwnym wypadku tworzyłby zagrożenie dla zrównoważonego rozwoju gospodarczego.

Na potrzeby niniejszego opracowania pojęcie „systemu finansowego" zdefiniować można jako *zbiór rynków, instytucji, przepisów ustawowych, regulacji i technik, dzięki którym przedmiotem obrotu są obligacje, akcje i inne papiery wartościowe; określane są stopy procentowe; oraz świadczone są usługi finansowe*[7]. Pod pojęciem tym można również rozumieć system złożony *z czterech ogniw: instrumentów finansowych; rynków finansowych; instytucji finansowych; zasad, na jakich działają trzy pierwsze ogniwa*[8]. Za instytucje finansowe uznać należy: banki, instytucje kredytowe, fundusze inwestycyjne, zakłady ubezpieczeń, fundusze emerytalne, a także domy maklerskie. Rynek finansowy podzielić można na: rynek pieniężny, kapitałowy, walutowy i instrumentów

---

[2] *The High-level Group of Financial Supervision in the EU, Chaired by Jacques de Larosiere, Final Report,* Brussels, 25 February 2009, http://ec.europa.eu/internal_market/finances/docs/de_larosiere_report_en.pdf [dostęp: 5.04.2019].

[3] *High-level Expert Group on Reforming the Structure of the EU Banking Sector, Chaired by Erkki Liikanen, Final Report*, Brussels, 2 October 2012.

[4] Independent Commission on Banking, *Final Report. Recommendations*, September 2011, http://www.ecgi.org/documents/icb_final_report_12sep2011.pdf [dostęp: 7.05.2019].

[5] *Financial Reform. A Framework for Financial Stability*, Group of Thirty, 15 January 2009, http://fic.wharton.upenn.edu/fic/Policy%20page/G30Report.pdf [dostęp: 7.05.2019].

[6] *A Reformed Financial Sector for Europe, Commission Staff Working Socument*, European Commission, Brussels, 15 May 2014, COM(2014)279 final, s. 22.

[7] P.S. Rose, M.H. Marquis, *Financial Institutions and Markets*, New York 2011.

[8] B. Pietrzak, Z. Polański, B. Woźniak, *System finansowy w Polsce*, Warszawa 2008, s. 17 i n.

pochodnych. Ważną rolę w zapewnieniu prawidłowego przebiegu procesów finansowych pełnią regulacje prawne oraz podmioty pełniące nadzór nad działalnością konkretnych instytucji i rynków finansowych. Należy jednocześnie zauważyć, że niewłaściwie prowadzony nadzór oraz przyjęcie błędnej strategii legislacyjnej są zjawiskami, które niezwalczane, prowadzić mogą do zjawisk niekorzystnych, w postaci różnego rodzaju kryzysów. Zasadniczo system finansowy pozwala na przepływ środków (pieniężnych) od podmiotów, które rozporządzają oszczędnościami (tj. nie wydają całości dochodów) do podmiotów, które są pożyczkobiorcami (tj. które nie są w stanie pokryć wydatków wyłącznie z dochodów). Przepływy finansowe dokonywane są na dwa sposoby:

- bezpośrednio – przez rynki finansowe,
- pośrednio – przez pośredników (zwykle banki).

Dla prawidłowego funkcjonowania systemu finansowego niezwykle ważna jest nowoczesna infrastruktura, zawierająca systemy płatności i rozliczeń transakcji instrumentami finansowymi, instytucje zwiększające przejrzystość (różnego rodzaju rejestry, np. kredytowe) oraz procedury ochrony uczestników rynku (np. systemy gwarantowania depozytów).

Rozwój systemu finansowego oraz umożliwienie pełniejszej realizacji jego funkcji pozwala na osiąganie ważnych celów ekonomicznych. System finansowy wypełnia niejako służebną rolę wobec innych sfer gospodarki. Jego głównym zadaniem jest zapewnienie dostępu do określonych usług innym podmiotom niefinansowym. W efekcie system finansowy, poprzez stwarzanie udogodnień proceduralnych oraz obniżanie kosztów związanych z prowadzeniem działalności, powinien przyczyniać się do wzrostu efektywności funkcjonowania innych sektorów gospodarki. Prowadzenie działalności w ramach rynku finansowego związane jest z różnego rodzaju kosztami. Z uwagi na ten fakt zasadniczą kwestią wydaje się zapewnienie wysokiej jakości świadczonych usług w taki sposób, aby zminimalizować występujące przy tym koszty (np. koszty pośrednictwa finansowego).

Faktem jest, że system finansowy w istotny sposób wpływa na przebieg procesów zachodzących w gospodarce. W konsekwencji system finansowy może mieć zarówno pozytywne, jak i negatywne skutki dla rozwoju gospodarczego. W przypadku nieprawidłowego funkcjonowania może to prowadzić do spowolnienia wzrostu gospodarczego.

1.2. Modele systemu finansowego

Omawiając pojęcie „systemu finansowego”[9], wskazać można dwa główne sposoby przepływu środków pieniężnych (od podmiotów dysponujących oszczędnościami do podmiotów będących pożyczkobiorcami), tj. finansowanie bezpośrednie, z wykorzystaniem rynków finansowych, i finansowanie pośrednie, z wykorzystaniem pośredników finansowych. Podział ten pozwala na wyodrębnienie dwóch modeli systemu finansowego[10]:

- zorientowanych rynkowo, w którym występuje przewaga finansowania bezpośredniego z wykorzystaniem rynków finansowych. Model ten bywa określany jako anglosaski, angloamerykański albo rynkowy. Upowszechnił się przede wszystkim w krajach takich jak Stany Zjednoczone i Wielka Brytania;
- zorientowanych bankowo, w którym występuje przewaga finansowania poprzez pośredników finansowych, najczęściej banki. System ten bywa określany jako kontynentalny lub bankowy. Do krajów, w których system ten się upowszechnił, należą przede wszystkim Niemcy i Japonia.

Wśród przedstawicieli Doktryny od wielu lat toczy się dyskusja na temat tego, który z modeli pozwala w sposób skuteczniejszy realizować zadania oraz funkcje systemu finansowego, a zwłaszcza, który model pozwala na najbardziej efektywny transfer funduszy od oszczędzających do inwestorów. W ramach prowadzonej dyskusji przytacza się zarówno argumenty o charakterze teoretycznym, jak i empirycznym.

Badając model systemu zorientowanego bankowo[11], wskazuje się na następujące zalety:

- Banki, jako wyspecjalizowane w ocenie potencjalnych kredytobiorców, są w stanie ograniczyć koszty związane z uzyskiwaniem informacji dotyczących przedsiębiorstw i projektów inwestycji. Instytucje te mogą więc doprowadzić do wzrostu oszczędności oraz dostępności kapitału w gospodarce. Skuteczna identyfikacja wartościowych projektów

[9] M. Sobol, *System finansowy a wzrost gospodarczy*, „Studia Ekonomiczne Prawne i Administracyjne” 2015, nr 2, s. 42–53.

[10] www.nbp.pl/systemfinansowy/rozwoj [dostęp: 5.05.2019].

[11] K. Hofman, *Banki zagraniczne w Europie środkowej. Wnioski z dotychczasowych doświadczeń*, Warszawa 2005, s. 82 i n.

i przedsiębiorstw sprzyja bowiem innowacyjności i efektywniejszej alokacji zasobów. Banki mają także wpływ na funkcjonowanie ładu korporacyjnego oraz są w stanie skuteczniej niż rynek kontrolować i egzekwować spłatę zobowiązań (chodzi głównie o udzielone kredyty);
- Banki przyczyniają się do ograniczenia ryzyka płynności przez gromadzenie oszczędności i inwestowanie ich w instrumenty krótkoterminowe oraz długoterminowe papiery wartościowe;
- Instytucje bankowe pozwalają również na dzielenie ryzyka pomiędzy indywidualnych inwestorów, co umożliwia realizowanie projektów o wyższej stopie zwrotu, ale i wyższym ryzyku;
- System bankowy umożliwia również mobilizację kapitału w celu skorzystania z efektu ekonomii skali.

W przypadku systemu opartego głównie na rynkach podkreślane są następujące korzyści:
- Płynność, właściwa rynkowi akcji, dostarcza inwestorom bodźców do inwestowania w pozyskiwanie i przetwarzanie informacji. Stanowi również istotną zachętę do realizowania zysków przez dokonywane na rynku transakcje;
- Rynek kapitałowy wpływa na poprawę alokacji zasobów i służy wzmocnieniu ładu korporacyjnego, co znacząco ułatwia procesy przejęć przedsiębiorstw oraz prowadzi do wynagradzania kadry zarządzającej w zależności od wyników uzyskiwanych przez spółki;
- Rozwinięte rynki wpływają również pozytywnie na zarządzanie ryzykiem finansowym, pozwalając zmniejszyć ryzyko płynności poprzez szybką sprzedaż instrumentów finansowych na rynkach bardziej płynnych;
- W omawianym systemie rynki finansowe służą również gromadzeniu rozproszonych informacji i przekazywaniu ich inwestorom, co ma pozytywny wpływ na finansowanie przedsiębiorstw oraz ich wyniki;
- Rynki sprzyjają także innowacyjności, poprzez lepsze finansowanie projektów o wysokim ryzyku i stopie zwrotu.

Oprócz wymieniania zalet związanych z danym modelem systemu finansowego zwolennicy obu systemów wskazują słabości modelu konkurencyjnego. Wśród wad systemu opartego na rynkach wymienia się najczęściej niedoskonałości mechanizmów rynkowych, skuteczniejsze realizowanie

przez banki kontroli korporacyjnej, ze względu na pełniejszy dostęp do wewnętrznej informacji przedsiębiorstw, a także skuteczniejsze narzędzia dywersyfikacji ryzyka. Zwolennicy tego systemu poddają krytyce sektor bankowy i wskazują na negatywny wpływ instytucji bankowych na realizację innowacyjnych projektów, nieskuteczne sprawowanie nadzoru korporacyjnego oraz niewielką w porównaniu do rynków ofertę instrumentów służących dywersyfikacji ryzyka oraz zabezpieczaniu się przed nim[12]. Dane uzyskane w wyniku przeprowadzonych badań empirycznych nie pozwalają na jednoznaczne wskazanie lepszego systemu. Analiza związków między systemem finansowym a wzrostem gospodarczym prowadzi bowiem jedynie do przekonania o znaczeniu ogólnego poziomu rozwoju systemu finansowego, a nie jego struktury[13]. Wyniki przeprowadzonych badań wskazują na ważną rolę jakości usług świadczonych przez system finansowy, a nie jego struktury. Duże znaczenie mają szczegółowe rozwiązania prawne. Wśród przedstawicieli doktryny prezentowane są różne poglądy dotyczące struktury systemu finansowego oraz wpływających na nią czynników. Wskazuje się między innymi na znaczenie uwarunkowań politycznych, kulturowych, geograficznych czy rozwiązań prawnych. W przypadku uwarunkowań prawnych podkreślić należy potrzebę rozróżnienia systemów opartych na tradycji anglosaskiej i systemów prawnych kontynentalnych. Kraje o anglosaskiej tradycji prawa charakteryzuje silna ochrona praw akcjonariuszy i wierzycieli, występowanie dobrych regulacji w zakresie rachunkowości, a także zorientowanie na rynek. Kraje o kontynentalnej tradycji prawa charakteryzują słabsza ochrona praw akcjonariuszy i wierzycieli, niskie standardy systemów księgowych, mniejsze zorientowanie na rynek oraz oparcie na bankach w znacznie większym stopniu. Należy również zauważyć, że rozwój finansowy, definiowany przez uprawnienia inwestorów w powiązaniu ze skutecznością systemu egzekwowania tych uprawnień, jest dodatnio związany z trwałym wzrostem gospodarczym. Powyższe spostrzeżenie pozwala stwierdzić, że system prawny jest istotnym czynnikiem mającym wpływ na rozwój systemu finansowego oraz w efekcie na wzrost gospodarczy.

---

[12] T. Beck, *Financial Development and Economic Growth. Stock Markets versus Banks?*, Tilburg 2010, s. 2 i n.

[13] R. Levine, *Bank-based or Market-based Financial Systems. Which is Better?*, „Journal of Financial Intermediation" 2002, vol. 11, s. 398–428.

Zauważyć jednak należy, że przeciwstawianie banków rynkom finansowym nie wydaje się w pełni uzasadnione. W rzeczywistości mamy bowiem na ogół do czynienia z połączeniem w różnych proporcjach obydwu sposobów finansowania podmiotów gospodarczych. Banki i rynki finansowe bardzo często się uzupełniają albo wspólnie rozwijają[14]. Możliwe jest wskazanie zależności:

- rozwinięty, płynny rynek akcji pozwala na równoważenie niekorzystnych skutków związanych ze znaczną przewagą banków nad przedsiębiorstwami;
- rynki finansowe i banki nie finansują tych samych segmentów przedsiębiorstw. Z kapitału uzyskanego na rynku akcji finansuje się najczęściej duże przedsiębiorstwa o długiej historii działania.

Analiza struktury międzynarodowego systemu finansowego pozwala wyróżnić grupy krajów, których systemy finansowe są oparte na rynkach albo na instytucjach bankowych[15]. Badanie systemów 27 krajów członkowskich UE pod kątem znaczenia w systemie finansowym banków i rynków oraz porównanie wyników badań z systemami Stanów Zjednoczonych oraz Japonii, przeprowadzone na podstawie 23 różnych wskaźników opisujących systemy finansowe, pozwala wyodrębnić cztery grupy państw:

- z systemami finansowymi zorientowanymi rynkowo – Holandia, Wielka Brytania, Belgia, Francja, Finlandia i Szwecja. Struktura systemów finansowych państw tej grupy wykazuje istotne podobieństwo do systemu finansowego Stanów Zjednoczonych;
- z systemami zorientowanymi bankowo – Austria, Dania, Niemcy, Grecja, Włochy, Portugalia i Hiszpania. Struktura finansowa tych krajów przywodzi na myśl system finansowy Japonii;
- kraje Europy Środkowo-Wschodniej – Bułgaria, Czechy, Estonia, Węgry, Łotwa, Litwa, Polska, Rumunia, Słowacja i Słowenia. Grupa

[14] F. Song, A.V. Thakor, *Financial System Architecture and the Co-evolution of Banks and Capital Markets*, „Economic Journal" 2010, vol. 120, s. 1021–1055.

[15] J. Allard, R. Blavy, *Market Phoenixes and Banking Ducks. Are Recoveries Faster in Market-Based Economies?*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.893.4840&rep=rep1&type=pdf [dostęp:15.04.2019]; M.J. Bijlsma, G.T.J. Zwart, *The Changing Landscape of Financial Markets in Europe, the United States and Japan*, http://bruegel.org/wp-content/uploads/imported/publications/WP_2013_02_01.pdf [dostęp: 14.05.2019].

ta obejmuje kraje, które przystąpiły do UE w 2004 r. lub 2007 r. Systemy finansowe tych krajów są, ogólnie rzecz biorąc, mniejsze niż krajów, które przystąpiły do UE przed 2004 r.

- pozostałe – Irlandia, Malta, Cypr, Luksemburg. Z uwagi na różne uwarunkowania, kraje te znacznie odstają od pozostałych, co uzasadnia ujęcie ich w oddzielnej grupie. System finansowy w tych państwach charakteryzuje się bardzo dużym sektorem bankowym oraz wysoką relacją wartości kredytów do PKB.

Kraje z systemami finansowymi zorientowanymi bankowo mieszczą się głównie w Europie Południowej i Centralnej. Nowe kraje członkowskie UE tworzą zaś oddzielną grupę pod względem specyfiki systemu finansowego. Kraje północno-zachodniej Europy charakteryzują się systemami finansowymi opartymi na rynkach[16], posiadając jednakże znaczne sektory bankowe. Najprawdopodobniej jest to efekt transgranicznej działalności banków mających swą siedzibę w tych krajach. Aktywa i zobowiązania zagraniczne instytucji bankowych są w tych państwach wyższe niż aktywa i zobowiązania w sąsiadujących krajach z systemami opartymi na bankach. Jako główną różnicę pomiędzy bankami we wskazanych państwach wskazać można ich źródła zysków. W pierwszej grupie z systemami finansowymi opartymi na rynkach źródłem większości dochodów banków są różnorakie opłaty i prowizje, nie zaś odsetki, w przeciwieństwie do systemów zorientowanych bankowo.

Nie ulega wątpliwości, że właściwie wypełniający swoje zadanie system finansowy powinien odznaczać się kompletnością i zróżnicowaniem[17]. Tylko w przypadku takiego systemu możliwe staje się osiąganie zysków wynikających z komplementarności oraz wzajemnego wspierania swojego rozwoju przez poszczególne segmenty tego rynku. Rozwiązanie takie służy również obniżeniu podatności systemu finansowego na zakłócenia stabilności, co umożliwia nie tylko uzyskanie lepszego wyniku finansowego działającym na nim podmiotom, ale także pozwala uniknąć niepotrzebnych strat.

[16] M. Górski, *Rynkowy system finansowy*, Warszawa 2018, s. 93 i n.
[17] S. Heffernan, *Nowoczesna bankowość*, Warszawa 2007, s. 19 i n.

1.3. Funkcje systemu finansowego

Podstawowym zadaniem systemu finansowego jest umożliwienie rozmieszczania zasobów gospodarczych zarówno w czasie, jak i w przestrzeni, w niepewnym otoczeniu[18]. Poza tą funkcją system finansowy powinien zapewniać[19]:

- **Wymianę wartości**. System płatniczy charakteryzujący się bezpieczeństwem i wysoką efektywnością ma podstawowe znaczenie dla funkcjonowania gospodarki. Zasadniczo powinien on zapewniać szybkość i terminowość rozrachunku transakcji. Powinien również być dostępny dla podmiotów mających potrzebę dokonania płatności oraz podmiotów mających płatność otrzymać; a także powinien umożliwiać skoordynowanie z innymi procesami gospodarczymi. Jako narzędzie łatwe i bezpieczne powinien także odznaczać się przystępnością i transparentnością, umożliwiając swoim użytkownikom uzyskanie potrzebnych informacji o dostępnych metodach płatności i związanych z nimi kosztami.
- **Pośrednictwo**. Przepływ środków pomiędzy oszczędzającymi i kredytobiorcami. System finansowy umożliwia podmiotom poszukującym źródeł finansowania uzyskanie środków od podmiotów oszczędzających. Ta funkcja systemu nie polega jedynie na udzielaniu kredytów oraz przyjmowaniu depozytów. Dobrym przykładem może być fakt pośredniczenia przez firmy inwestycyjne pomiędzy emitentami papierów wartościowych a inwestorami. Charakter czynności ma decydujące znaczenie dla faktu, czy omawiane pośrednictwo obejmuje także funkcje uzupełniające, takie jak łączenie zasobów, co umożliwia sfinansowanie przy pomocy stosunkowo niewielkich depozytów kredytu o znacznej wartości. Wśród funkcji pomocniczych wyróżnić należy dodatkowo transformację terminów; funkcję oceny ryzyka i przetwarzania informacji (w tym np. analizowanie potencjalnych

[18] R.C. Merton, *Operation and Regulation in Financial Intermediation. A Functional Perspective*, Stockholm 1993, s. 17–68.

[19] *Submission to the Financial System Inquiry*, March 2014, Reserve Bank of Australia, http://www.rba.gov.au/publications/submissions/fin-sys-inquiry-201403/pdf/fin-sys-inquiry-201403.pdf [dostęp: 5.04.2019]; *Policy Framework for Effective and Efficient Financial Regulation*, Paris 2010, s. 15–18.

kredytobiorców umożliwiające identyfikację okazji do zyskownego rozwoju akcji kredytowej oraz monitorowanie wszystkich dłużników mające na celu obniżenie ryzyka niespłacenia udzielonego kredytu. W procesie pośrednictwa istotne znaczenie ma także efektywne rozdysponowanie środków, przejawiające się w nakierowaniu środków finansowych na te przedsięwzięcia, co do których istnieje przekonanie o ich wysokiej efektywności. Poprzez omówione funkcje system finansowy służy wzrostowi potencjału wytwórczego gospodarki oraz ma wpływ na podniesienie poziomu życia.

- **Transfer ryzyka**. Efektywny system finansowy umożliwia również skuteczne zarządzanie różnymi rodzajami ryzyka, np. kredytowym, rynkowym, ubezpieczeniowym, a także operacyjnym. Podkreślenia wymaga fakt, iż nie jest rolą systemu finansowego całkowite wyeliminowanie ryzyka – nie jest to zadanie możliwe do zrealizowania. Wskazać również należy, że takie działanie wpłynęłoby negatywnie na przedsiębiorczość oraz na innowacyjność gospodarki. Celem efektywnego systemu finansowego powinien być zamiast tego transfer ryzyka związanego z działalnością instytucji rynku finansowego do podmiotów, które są z racji prowadzonej działalności najlepiej przygotowane do zarządzania różnymi formami ryzyka.
- **Płynność**. Niezwykle istotnym zadaniem systemu finansowego jest zapewnienie płynności instytucji finansowych. Należy podkreślić, że jeżeli system ten funkcjonuje prawidłowo, to umożliwia on podmiotom gospodarczym szybką zamianę swoich aktywów w gotówkę, bez nieuzasadnionej utraty wartości.

System finansowy powinien również udostępniać podmiotom działającym na rynkach finansowych informacje na temat możliwych projektów inwestycyjnych oraz, po zapewnieniu im finansowania, umożliwiać monitorowanie tych projektów oraz kontrolę przestrzegania ładu korporacyjnego[20].

W literaturze przedmiotu wyróżnia się także inne klasyfikacje tych funkcji. Wśród nich wskazać należy podział zadań pełnionych przez system finansowy na[21]:

---

[20] R. Levine, *Finance and Growth. Theory and Evidence*, Amsterdam 2005, s. 872 i n.

[21] B. Pietrzak, Z. Polański, B. Woźniak, *op. cit.*

- **monetarną**. Zgodnie z nią zadaniem systemu jest zapewnienie dostaw pieniądza do gospodarki oraz stworzenie możliwości jego obiegu. System finansowy pełni zatem rolę płatniczą, rolę gwarancji płynności oraz odpowiada za kreację pieniędzy.
- **kapitałowo-redystrybucyjną**. Istotą tej funkcji jest zapewnienie swobodnego przepływu wolnych środków pieniężnych, ograniczenie ryzyka oraz transformacja terminów, na jakie te fundusze są pożyczane przez instytucje finansowe.
- **kontrolną**. Funkcja ta opiera się na zapewnieniu kontroli nad strumieniami pieniężnymi, zwłaszcza nad środkami już zainwestowanymi. Ma zatem dostarczyć narzędzi umożliwiających kontrolę efektywności wykorzystania aktywów.

Uczestnicy systemu rynku finansowego (tj. państwo i inne podmioty), dokonując transakcji, są odpowiedzialni za przepływ środków finansowych od podmiotów oszczędzających do podmiotów odczuwających brak kapitału[22]. Na system rynków finansowych składają się m.in. rynek bankowy, kapitałowy oraz ubezpieczeń, na których to rynkach działają z kolei różnorakie podmioty sektora finansowego. Według Systemu Rachunków Narodowych i Regionalnych ESA 2010 można wyróżnić następujące podmioty należące do rynku finansowego:

1. Bank centralny,
2. Instytucje przyjmujące depozyty, z wyjątkiem banku centralnego,
3. Fundusze rynku pieniężnego,
4. Fundusze inwestycyjne, niebędące funduszami rynku pieniężnego,
5. Pozostałe instytucje pośrednictwa finansowego, z wyjątkiem instytucji ubezpieczeniowych i funduszy emerytalno-rentowych,
6. Pomocnicze instytucje finansowe,
7. Instytucje finansowe typu captive i udzielające pożyczek,
8. Instytucje ubezpieczeniowe,
9. Fundusze emerytalno-rentowe.

W Polsce wskazać można przede wszystkim: banki komercyjne z oddziałami zagranicznymi, fundusze emerytalne i powszechne towarzystwa emerytalne, banki spółdzielcze, zakłady ubezpieczeń osobowych i majątkowych,

[22] J. Czekaj, *Rynki, instrumenty i instytucje finansowe*, Warszawa 2019, s. 7 i n.

zakłady ubezpieczeń na życie, domy maklerskie, spółdzielcze kasy oszczędnościowo-kredytowe, towarzystwa funduszy inwestycyjnych.

Transakcje rynkowe przekładają się na bardziej efektywne wykorzystywanie zasobów w gospodarce oraz prowadzą do wspierania projektów nastawionych na rozwój i inwestycje o dużej wartości. Efektywny rynek finansowy służy optymalizacji procesów inwestycyjnych, w efekcie prowadzi do szybszego wzrostu gospodarczego. Pełni również rolę mobilizacyjną, gdyż umożliwia, jak już wspomniano, przepływ nadwyżki środków finansowych do podmiotów poszukujących źródeł finansowania. Pozwala również na wycenę kapitału poprzez dostarczenie inwestorom informacji o wartości inwestycji i pełni funkcję prognostyka koniunktury gospodarczej. Sprawny i uporządkowany rynek finansowy ma więc fundamentalne znaczenie dla procesu podejmowania decyzji w instytucji finansowej, gdyż umożliwia uzyskanie podmiotom decyzyjnym sprawdzonych, kompletnych informacji, które są niezbędne dla trafnego przewidywania zmian koniunktury oraz minimalizacji ryzyka związanego z podejmowanymi działaniami.

1.4. Rodzaje rynku finansowego i jego uczestnicy

W ramach rynku finansowego najczęściej wyróżnia się:

- rynek pieniężny – dotyczy on transakcji o okresie zapadalności nie dłuższym niż rok,
- rynek kapitałowy – dotyczy on transakcji, dłuższym niż rok okresie zapadalności,
- rynek terminowy – dotyczy obrotu instrumentami pochodnymi, przy wykorzystaniu dźwigni finansowych,
- rynek walutowy,
- rynek depozytowo-kredytowy.

Uczestnikami rynku finansowego oprócz podmiotów prywatnych są Skarb Państwa oraz Narodowy Bank Polski i Komisja Nadzoru Finansowego[23]. Najistotniejszym zadaniem NBP w zakresie rynku finansowego jest przygotowywanie w „Raportach o stabilności systemu Finansowego" oceny

[23] *Ibidem.*

sytuacji polskiego systemu finansowego, analiza głównych ryzyk ekonomicznych, na które narażone są instytucje finansowe, oraz przedstawienie analizy odporności instytucji finansowych na różnego rodzaju ryzyka. Komisja Nadzoru Finansowego współpracuje natomiast z unijnymi instytucjami nadzoru finansowego, mając za zadanie sprawowanie ciągłej kontroli ryzyka, na jakie narażone są podmioty rynku finansowego oraz metod zarządzania tym ryzykiem, przyjmowanych przez poszczególne podmioty. Wśród instytucji, z którymi współpracuje KNF, wymienić należy EBA (ang. *European Banking Authority*), ESMA (ang. *European Securities and Markets Authority*) oraz EIOPA (ang. *European Insurance and Occupational Pensions Authority*), jak również globalnych organizacji zrzeszających organy nadzoru, w tym IOSCO (ang. *International Organization of Securities Commissions*) i IAIS (ang. *International Association of Insurance Supervisors*).

W roli uczestnika systemu rynku finansowego może również występować państwo, a także inne podmioty publiczne, dokonując operacji mających na celu przesunięcia środków pieniężnych od podmiotów posiadających oszczędności do podmiotów, którym brakuje środków na zaspokojenie ich potrzeb. Podmioty te pełnią jednak przede wszystkim funkcje regulatora oraz nadzorcy systemu. Wpływają na koniunkturę gospodarczą oraz na stabilność systemu finansowego, stosując różnego rodzaju narzędzia oraz instrumenty z zakresu nadzoru makrooszczędnościowego, polityki fiskalnej, pieniężnej i walutowej na podmioty działające na rynku, respektując zasady ograniczonego i uzasadnionego zakresu ingerowania państwa w mechanizmy rynkowe. Działania zmierzające do stabilizacji sytuacji finansowej mają na celu wspieranie rozwoju gospodarczego.

Działanie rynków finansowych regulowane jest w Polsce szczegółowo metodą ustawową oraz za pomocą aktów nadzoru finansowego. Celem działań ustawodawczych jest ochrona inwestorów, zapewnienie równowagi rynkowej, działanie na rzecz uczciwości obrotu, przeciwdziałanie ryzyku systemowemu, a także działanie na rzecz konkurencji rynkowej. Jednym z najważniejszych podmiotów publicznych, oddziałujących na rynki bankowe, kapitałowe i ubezpieczeniowe za pomocą aktów nadzoru finansowego oraz różnego rodzaju środkami miękkimi, jest Komisja Nadzoru Finansowego. Na rynki finansowe wpływa też Narodowy Bank Polski, przede wszystkim przez organ, jakim jest Rada Polityki Pieniężnej, do zadań której należy ustalanie

wysokości stóp procentowych. Rolę regulacyjną pełni również Komisja Europejska wraz z innymi podmiotami unijnymi[24].

1.5. Instytucje finansowe

Zgodnie z ustawą[25] instytucja finansowa jest odrębnym podmiotem działającym na rynku finansowym, niebędąca bankiem ani instytucją kredytową. Jej podstawową działalnością, stanowiącą źródło większości przychodów, jest wykonywanie działalności gospodarczej w zakresie uregulowanym przepisami prawa bankowego (rozdz. 1 art. 4 pkt 7 ustawy prawo bankowe). Zgodnie jednak z poglądem powszechnym w doktrynie należy uznać, że pojęcie to ma znaczenie szersze, niż mogłoby się to wydawać na podstawie wykładni literalnej ustawy. Pod terminem tym należałoby raczej rozumieć podmioty aktywne na rynku finansowym, mające w swym portfelu przeważający udział aktywów finansowych[26]. Wśród instytucji finansowych wyróżnić można zatem instytucje bankowe, kasy oszczędnościowe i kredytowe, a także niebankowe instytucje finansowe, do których zalicza się m.in. fundusze emerytalne, fundusze inwestycyjne, firmy ubezpieczeniowe czy domy maklerskie[27].

Należy zauważyć, że działalność instytucji finansowych na rynku ma wiele pozytywnych efektów, takich jak[28]:

- rozwój strategii zmniejszania ryzyka podejmowanych decyzji,
- usprawnianie systemu transakcyjnego,
- pobudzanie popytu,
- organizowanie źródeł i sposobów zasileń kapitałowych podmiotów gospodarczych,
- poprawa warunków bezpieczeństwa.

---

[24] Z. Jurkowska-Zeidler, *Bezpieczeństwo rynku finansowego w świetle prawa Unii Europejskiej*, Warszawa 2008.

[25] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, Dz.U. 1997 Nr 140, poz. 939 t.j.

[26] D. Korenik, *Innowacyjne usługi banku*, Warszawa 2006.

[27] Z. Dobosiewicz, *Bankowość*, Warszawa 2003, s. 16 i n.

[28] S. Smyczek, *Modele zachowań konsumentów na rynku usług finansowych*, Katowice 2007, s. 98 i n.

Wśród instytucji finansowych możliwe wydaje się wyróżnienie następujących grup[29]:

- instytucje wspomagające działalność przedsiębiorstw finansowych i zmniejszające ryzyko finansowe i techniczne operacji (Krajowa Izba Rozliczeniowa, Krajowy Depozyt Papierów Wartościowych, Ubezpieczeniowy Fundusz Gwarancyjny, TUW SKOK, KUKE, Bankowy Fundusz Gwarancyjny, fundacje, instytucje szkoleniowe, zrzeszenia branżowe),
- instytucje zajmujące się pośrednictwem finansowym (banki, fundusze emerytalne, firmy leasingowe oraz factoringowe, zakłady ubezpieczeniowe, biura maklerskie, fundusze inwestycyjne i powiernicze, giełdy papierów wartościowych, spółdzielcze kasy oszczędnościowo-kredytowe),
- instytucje sprawujące nadzór nad określonymi segmentami rynków finansowych (Komisja Nadzoru Bankowego, Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa)[30].

Druga grupa instytucji finansowych – pośredników finansowych ma istotne znaczenie dla rynku finansowego. Instytucje te zasilają w wyniku przeprowadzanych operacji, w sposób bezpośredni bądź pośredni, pozostałych członków rynku w kapitał pieniężny, który jest niezbędny do ich prawidłowego funkcjonowania i rozwoju, a także do zapewnienia im gwarancji zabezpieczenia w przypadku niepowodzenia przedsięwzięcia[31]. Zarówno te podmioty, jak i dokonywane przez nie operacje będą przedmiotem pogłębionej analizy w dalszej części tekstu.

Podziału drugiej grupy instytucji finansowych można również dokonać ze względu na rodzaj danej instytucji[32]. Jest to podział jasny i pozwalający wskazać możliwie dużą liczbę podmiotów. Można zatem wyróżnić:

- instytucje bankowe, do których zalicza się wszelkiego rodzaju banki (komercyjne oraz spółdzielcze);

---

[29] M. Górski, *op. cit.*

[30] A. Jakubowska, *Funkcjonowanie gospodarki polskiej po 20 latach transformacji*, Szczecin 2009, s. 160–171.

[31] F.S. Mishkin, S.G. Eakins, *Financial Markets and Institutions*, Boston 2015, s. 134–190.

[32] M. Capiga, G. Szustak, *Zarządzanie instytucjami finansowymi w niestabilnym otoczeniu gospodarczym*, Katowice 2014, s. 120 i n.

- instytucje parabankowe, do których zaliczyć można spółdzielcze kasy oszczędnościowo-kredytowe (SKOK-i), firmy leasingowe, firmy factoringowe, pośredników i krokerów finansowych,
- instytucje niebankowe, takie jak fundusze inwestycyjne, fundusze emerytalne, towarzystwa ubezpieczeniowe, domy i biura maklerskie, fundusze poręczeń kredytowych.

Z uwagi na jasność i zupełność wspomnianego kryterium podział dokonany stanowi podstawę analizy operacji dokonywanych przez instytucje finansowe.

1.6. Instytucje bankowe i ich operacje

Zgodnie z definicją zaczerpniętą z art. 2 ustawy prawo bankowe bank rozumiany jest jako osoba prawna utworzona zgodnie z przepisami ustaw, działająca na podstawie zezwoleń uprawniających do wykonywania czynności bankowych obciążających ryzykiem środki powierzone pod jakimkolwiek tytułem zwrotnym. Przytoczona definicja jest zgodna z definicją instytucji kredytowej zawartą w rozporządzeniu Parlamentu Europejskiego i Rady Unii Europejskiej nr 575/2013 z 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych.

W ustawie prawo bankowe zawarty jest zamknięty katalog czynności bankowych – określanych na ogół terminem „operacji”[33]. Cechą charakterystyczną czynności bankowych jest fakt ich skierowania na zewnątrz, do sfery stosunków bank – inny podmiot. Banki dokonują operacji we własnym interesie (np. lokaty pieniężne w innych bankach) lub w interesie innych osób (np. prowadzenie rachunków bankowych). Operacje łączą w sobie elementy czynności prawnej i faktycznej, mogą wyrażać kompleks umów bankowych (np. akredytywa dokumentowa), jedną umowę (np. kredyt hipoteczny) lub oznaczoną czynność w ramach umowy łączącej bank z klientem (np. dokonanie konkretnego rozliczenia)[34].

[33] H. Gronkiewicz-Waltz, M. Wierzbowski, *Prawo gospodarcze*, Warszawa 2017, s. 251 i n.
[34] M. Bączyk,*Umowy banku z jednostkami gospodarki uspołecznionej*, Toruń 1984.

Czynności bankowe *sensu stricto* wymienia art. 5 ust. 1 prawo bankowe:

- przyjmowanie wkładów pieniężnych płatnych na żądanie lub z nadejściem oznaczonego terminu oraz prowadzenie rachunków tych wkładów,
- prowadzenie innych rachunków bankowych,
- udzielanie kredytów,
- udzielanie i potwierdzanie gwarancji bankowych oraz otwieranie i potwierdzanie akredytyw,
- emitowanie bankowych papierów wartościowych,
- przeprowadzanie rozliczeń pieniężnych,
- wykonywanie innych czynności przewidzianych wyłącznie dla banku w odrębnych ustawach.

Pozostałe czynności, wymienione w art. 5 ust. 2, mogą być wykonywane również przez inne podmioty – są jednak również zaliczane do operacji bankowych, jeśli wykonują je banki:

- udzielanie pożyczek pieniężnych,
- operacje czekowe i wekslowe oraz operacje, których przedmiotem są warranty,
- świadczenie usług płatniczych oraz wydawanie pieniądza elektronicznego,
- terminowe operacje finansowe,
- nabywanie i zbywanie wierzytelności pieniężnych,
- przechowywanie przedmiotów i papierów wartościowych oraz udostępnianie skrytek sejfowych,
- prowadzenie skupu i sprzedaży wartości dewizowych,
- udzielanie i potwierdzanie poręczeń,
- wykonywanie czynności zleconych związanych z emisją papierów wartościowych,
- pośrednictwo w dokonywaniu przekazów pieniężnych oraz rozliczeń w obrocie dewizowym,
- pośrednictwo w zawieraniu umów lokaty strukturyzowanej,
- doradztwo w odniesieniu do lokat strukturyzowanych.

Próbując dokonać klasyfikacji operacji bankowych, najczęściej sięga się po tzw. klasyczny podział operacji bankowych na aktywne, pasywne i pośredniczące. Sprowadza się on do wyróżnienia strony aktywnej (chodzi

tu głównie o kredyty) i pasywnej (np. depozyty). Wskazać jednak należy, iż operacje instytucji finansowych mają często charakter zarówno pasywny, jak i aktywny. Istnieją również operacje nieodzwierciedlane bezpośrednio w bilansach bankowych (np. niektóre operacje papierami wartościowymi).

W świetle powyższych rozważań zasadne jest sformułowanie podziału uwzględniającego wzajemny stosunek pomiędzy instytucją a jej klientem[35]:

- usługi finansujące – wszystkie operacje, które prowadzą do natychmiastowego (lub w ustalonym późniejszym terminie) zwiększenia środków płatniczych klienta,
- usługi depozytowe – czyli operacje, które umożliwiają klientowi przekazanie bankowi czasowo niepotrzebnych mu środków w celu ich wykorzystania na rzecz osób trzecich na cele inwestycyjne czy konsumpcyjne,
- usługi związane z obsługą obrotu płatniczego – polegają na realizacji zleceń klienta wykonywania określonych operacji na rachunkach bankowych bądź są to operacje płatnicze dokonywane z inicjatywy samego banku,
- usługi różne – obejmują wiele rozmaitych usług oferowanych klientom przez banki (np. doradztwo, pośrednictwo w operacjach papierami wartościowymi itp.).

1.7. Instytucje regulujące i nadzorujące

Podmiotami pełniącymi funkcje nadzorczą oraz regulacyjną są między innymi: Komisja Nadzoru Finansowego, Narodowy Bank Polski, a także Ministerstwo Finansów. KNF została wyposażona w uprawnienia polegające między innymi na prowadzeniu rejestrów pośredników kredytowych oraz instytucji pożyczkowych. Warunkiem prowadzenia podobnej działalności jest uzyskanie wpisu do rejestru. W wypadku prowadzenia działalności polegającej na pośrednictwie oraz udzielaniu kredytów konsumenckich organowi nadzoru przysługuje prawo do odmowy dokonania wpisu do rejestru podmiotów niespełniających wymogów ustawowych. Nadzorem objęta jest

[35] *Bank und Börsenwesen*, red. M. Bitz, München 1981.

również działalność alternatywnych spółek inwestycyjnych (ASI). Zgodnie z przepisami przejściowymi podmioty te mogły warunkowo działać na dotychczasowych zasadach, aż do uzyskania wpisu do odpowiedniego rejestru lub do czasu uzyskania odpowiedniego zezwolenia na wykonywanie działalności. Podmioty te były więc zobowiązane do złożenia do KNF odpowiednich wniosków w celu uzyskania wymaganego wpisu lub zezwolenia. Narodowemu Bankowi Polskiemu od 8 lutego 2017 r. przekazano zadanie prowadzenia nadzoru systemowego nad działaniem schematów płatniczych. Podmioty, takie jak: instytucje prowadzące systemy płatności, schematy płatnicze, centralny depozyt papierów wartościowych oraz systemy rozliczeń i rozrachunku papierów wartościowych, zobowiązane zostały za pomocą różnego rodzaju obowiązków sprawozdawczych do poddania się działalności kontrolnej NBP.

Wymienione podmioty pełniące rolę regulatorów oraz nadzorców krajowego systemu finansowego we współpracy z Bankowym Funduszem Gwarancyjnym stanowią podstawy sieci bezpieczeństwa finansowego w ramach Komitetu Stabilności Finansowej. Wskazać należy, że w 2017 r. odbyło się pięć posiedzeń Komitetu w formule makroostrożnościowej (KSF-M). Na czterech z nich Komitet skierował do Ministra Rozwoju i Finansów rekomendację dotyczącą utrzymania antycyklicznego bufora kapitałowego[36] na poziomie 0%. Na posiedzeniu w grudniu 2017 r. wydana została, na wniosek KNF, opinia w sprawie uznania zidentyfikowanych przez KNF dwunastu banków krajowych za tzw. inne instytucje o znaczeniu systemowym (*Other Systemically Important Institution*)[37] oraz o zastosowaniu w stosunku do nich odpowiedniego bufora kapitałowego[38]. Komitet zaproponował również rekomendację na temat restrukturyzacji portfela kredytów mieszkaniowych

[36] http://www.nbp.pl/nadzormakroostroznosciowy/bufor.aspx [dostęp: 9.05.2019].

[37] O-SII – instytucja o znaczeniu systemowym inna niż globalna instytucja systemowo ważna (*Global Systemically Important Institution*, *G-SII*). Pojęcie tzw. innej instytucji o znaczeniu systemowym zostało wprowadzone do ustawy z dnia 5 sierpnia 2015 r. o nadzorze makroostrożnościowym nad systemem finansowym i zarządzaniu kryzysowym w systemie finansowym w związku z koniecznością zaimplementowania do polskiego porządku prawnego przepisów dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniającej dyrektywę 2002/87/WE i uchylającej dyrektywy 2006/48/WE i 2006/49/WE (Dz.Urz. UE L176 z 2013 r., s. 338) z późn. zm.

[38] http://www.nbp.pl/nadzormakroostroznosciowy/insrtumenty.aspx [dostęp: 9.05.2019].

w walutach obcych[39]. W jej skład wchodzą skierowane do poszczególnych podmiotów współpracujących z komitetem zalecenia, których wdrożenie miałoby umożliwić restrukturyzację walutowych kredytów mieszkaniowych poprzez porozumienie banków i klientów. Zauważyć należy, że przy ministrze właściwym do spraw instytucji finansowych funkcjonuje również Rada Rozwoju Rynku Finansowego. Organ ten pełni funkcję doradczą oraz opiniodawczą w zakresie spraw związanych z rozwojem i unormowaniem rynku finansowego.

[39] http://www.nbp.pl/nadzormakroostroznosciowy/podstawa/20170602.pdf [dostęp: 9.05.2019].

ROZDZIAŁ DRUGI

Rozwiązania organizacyjne ułatwiające zachowanie kontroli instytucji finansowej nad operacjami realizowanymi przez jej pracowników

2.1. Wprowadzenie

Propozycje zmian legislacyjnych przedstawione poniżej zostały uporządkowane według znaczenia dla kryminalnego porządku prawnego. Na początku tej części przedmiotem opracowania będzie zmiana charakteru prawnego rekomendacji i wytycznych Komisji Nadzoru Finansowego. Zaproponowane zostanie podniesienie rangi tych regulacji jako instrukcji określających sposób postępowania z chronionym dobrem prawnym w działalności instytucji finansowej. W ten sposób zostaną silnie powiązane z materialnym prawem karnym, gdyż ich przestrzeganie potencjalnie będzie prowadziło do niemożności pociągnięcia potencjalnego sprawcy przestępstwa (pracownika instytucji finansowej) do odpowiedzialności karnej z uwagi na pierwotną legalność czynu i brak naruszenia normy sankcjonowanej (wyłączenie bezprawności czynu będącej jedynym z elementów konstytutywnych przestępstwa). Stanowi to swoistą alternatywę dla działalności wewnętrznych departamentów zarządzania ryzykiem prawnym i komórek ds. ogólnego *compliance*, których zadaniem jest raczej reagowanie na negatywne bodźce, niż zachęcanie do przestrzegania rekomendacji zawartych w wewnętrznych regulacjach banku, będących odzwierciedleniem rekomendacji KNF.

W drugiej części poruszona zostanie kwestia szczególnej jednostki organizacyjnej do spraw zgodności działań instytucji finansowej z prawem karnym. Celem takiej organizacji będzie przeciwdziałanie przestępczości pracowników oraz zapewnienie spójnej i efektywnej struktury wewnętrznego nadzoru. Jest to zatem kolejny etap działań prewencyjnych instytucji

finansowych, które wdrażając odpowiednie mechanizmy prawne, mają nie tylko przeciwdziałać, ale też uniknąć potencjalnej odpowiedzialności za kryminalne czyny pracownika, którym nie udało się zapobiec albo wykryć we wczesnych formach stadialnych.

W trzeciej części poruszona zostanie kwestia pozycji prawnej sygnalistów zatrudnionych w instytucjach finansowych jako instrumentu inicjującego oddolną inicjatywę przeciwdziałania i reagowania na przestępczość pracowników instytucji finansowych. Omówiona zostanie struktura wewnętrzna oraz zewnętrzna mechanizmu sygnalizowania i jej wpływ na efektywną organizację Criminal Compliance oraz wykrywalność przestępstw.

Ostatnia część będzie dotyczyła nowelizacji Kodeksu karnego w artykule 304, związanym z wykorzystywaniem przymusowego położenia do obciążania drugiej strony stosunku prawnego nieekwiwalentnymi obowiązkami. Rewizja brzmienia tego przepisu w drodze dodania nowego znamienia typu czynu zabronionego na wzór regulacji wyzysku (art. 388) w Kodeksie cywilnym (wykorzystywanie niedoświadczenia lub niedołęstwa drugiej strony) będzie wiązała się z rolą prewencji ogólnej prawa karnego, która ma przeciwdziałać zjawisku *moral hazard* i skłaniać pracowników instytucji finansowych do zachowywania służebnej roli w stosunkach z klientem oraz utożsamiania interesu własnego i instytucji finansowej z jego interesem.

2.2. Zmiana charakteru prawnego rekomendacji Komisji Nadzoru Finansowego oraz ich wpływ na reguły postępowania z dobrem i bezprawność czynu

Charakter zmian: nowelizacja istniejących aktów prawnych
Obszar zmian: Kodeks karny, prawo bankowe, ustawa o nadzorze nad rynkiem finansowym

Tezy:

1. Należy ustalić charakter prawny rekomendacji Komisji Nadzoru Finansowego, tak by nie było najmniejszych wątpliwości, że choć można je zaliczyć do *soft law*, to powinny być przestrzegane przez członków

rynku finansowego, z powodu konsekwencji nieprzestrzegania i przestrzegania w obszarze prawa stanowionego.

2. Kodeks karny będzie odsyłać do norm i zaleceń zawartych w rekomendacjach oraz do wytycznych jako norm statuujących zasady postępowania z dobrem. Rolą takiego odesłania będzie wskazanie zasad postępowania z dobrem, których naruszenie wiąże się z zakwalifikowaniem czynu jako bezprawnego[40]. Będzie to bodziec skłaniający do stosowania się do zaleceń podmiotu nadzorującego zarówno przez organizacje finansowe, jak i przez ich pracowników.
3. Należy rozważyć wdrożenie mechanizmu, który będzie neutralizować ewentualne niedoskonałości (zdaniem podmiotów nadzorowanych) rekomendacji, opartego na regule *comply or explain*[41], która pozwoli na niezastosowanie się instytucji finansowej do rekomendacji i pierwotną legalność czynu pod warunkiem, że sprawca potencjalnego czynu uzasadni nieprzestrzeganie procedur i wykaże, że jego zachowanie było zgodne z regułami postępowania z chronionym dobrem. Dla implementacji takiego rozwiązania niezbędne będzie założenie, że rekomendacje nie są prawem stanowionym, ale *soft law*.
4. Zachętą do przestrzegania rekomendacji i wytycznych wydanych przez Komisję Nadzoru Finansowego będzie pierwotna legalność czynu pod warunkiem, że będzie z nimi zgodny.

Uzasadnienie:
Charakter prawny rekomendacji Komisji Nadzoru Finansowego budzi szereg kontrowersji w doktrynie. Pierwsza z nich dotyczy kwalifikacji tych aktów prawnych w hierarchii aktów prawnych. Część opracowań zawiera kwalifikację rekomendacji jako aktów wewnętrznie obowiązujących[42], które są przedmiotem kontroli sądowej. Inne zaś wskazują na niewiążący charakter tych aktów. Orzecznictwo natomiast jednoznacznie wypowiadało się o tych

[40] Nienaruszenie reguł postępowania z dobrem prawnym uniemożliwia zakwalifikowanie danego czynu jako bezprawnego kryminalnie.

[41] Por. https://www.cbr.cam.ac.uk/fileadmin/user_upload/centre-for-business-research/downloads/working-papers/wp407.pdf [dostęp: 8.12.2018].

[42] U podstaw takiej tezy tkwi założenie, że między Komisją Nadzoru Finansowego a nadzorowanymi podmiotami istnieje stosunek podległości.

regulacjach jako aktach wewnętrznie obowiązujących, lecz po zmianach strukturalnych w nadzorze nad rynkiem finansowym prawodawca nie przesądził, jaki charakter mają rekomendacje i wytyczne. Nawet gdyby jednak przyjąć ciągłość orzecznictwa w sprawie charakteru prawnego tych działań, to prawo sądowe nie stanowi źródła prawa w polskim porządku prawnym i niepewność, czy jednak istnieje obowiązek przestrzegania rekomendacji, tworzy znaczne ryzyko systemowe. I choć w Niemczech czy Wielkiej Brytanii takie rekomendacje nie mają charakteru wiążącego i organy nadzorcze pozostawiają w gestii podmiotów działających na rynku finansowym decydowanie o aplikowaniu ich, to można dostrzec odmienny od polskiego akcent zorientowany na ich przestrzeganie, choćby poprzez obowiązek uzasadnienia niewdrożenia rekomendacji w oparciu o mechanizm *comply or explain*.

Należy więc zastanowić się, jaki status prawny powinny mieć wspominane wyżej rekomendacje. Jeżeli przyjąć, że nie stanowią one źródła prawa wewnętrznie obowiązującego, to trudno spójnie uzasadnić możliwość nakładania sankcji przez KNF za ich nieprzestrzeganie[43]. Zakwalifikowanie ich do kategorii prawa wewnętrznego przyniosłoby więcej korzyści i byłoby bliższe rzeczywistości niż odmienne koncepcje. Przede wszystkim przepisy wewnętrznie obowiązujące są źródłem prawa w rozumieniu Konstytucji i podlegają sądowej kontroli. To już stawia adresatów takich aktów w silniejszej pozycji prawnej. Ponadto, takie podniesienie rangi i doniosłości aktu sprawia, że ich wydawanie będzie wymagało uprzednich konsultacji z branżą, bowiem jako przepisy, do wykonywania których instytucje finansowe będą zobowiązane, mogą mieć ogromne znaczenie dla działalności operacyjnej instytucji finansowych. Tak jak w zwykłej procedurze prawodawczej istnieje miejsce na lobbing, tak będzie w tym przypadku. Szczególnie że organ nadzoru musi balansować w swoich działaniach właściwych dla prawa publicznego, musi respektować przepisy prawa prywatnego i swobodę działalności gospodarczej. Jednoznaczna decyzja w sprawie kwalifikacji rekomendacji jako aktów wewnętrznie obowiązujących wpłynie pozytywnie na gwarancje prawne podmiotów nadzorowanych.

Bez względu jednak na ewentualną ingerencję ustawodawcy, rekomendacje Komisji Nadzoru Finansowego powinny pozostawać w bliższej relacji

[43] Przykładem takiej kompetencji jest art. 138 ust. 7a ustawy prawo bankowe.

z gospodarczym prawem karnym, a nie pozostać wyłącznie domeną prawa administracyjnego. Celem takich rekomendacji jest bowiem przedstawienie instytucjom finansowym sposobu zachowania w określonych sytuacjach. Te instrukcje wydawane przez organ nadzorczy mają na celu ochronę określonych dóbr prawnych (np. stabilności systemu finansowego czy interesów gospodarczych obywateli). Przekładając to założenie na matrycę elementów konstrukcyjnych przestępstwa, należy się zastanowić, czy przestrzeganie standardów określonych przez organ nadzorczy nie skłania do zakwestionowania bezprawności potencjalnego przestępstwa pracowników instytucji finansowej. Jeżeli bowiem przyjmiemy, że elementem konstrukcyjnym przestępstwa jest bezprawność czynu[44], to nawet zachowanie pracowników instytucji finansowej sprowadzające niebezpieczeństwo na dobro prawne, ale nienaruszające reguł postępowania z dobrem prawnym wiążącym w danych okolicznościach sprawia, że czyn jest pierwotnie legalny i nie można potencjalnemu sprawcy przypisać odpowiedzialności karnej.

We włoskich regulacjach związanych z okolicznościami ograniczającymi albo wyłączającymi ewentualną odpowiedzialność za przestępstwa popełnione przez pracowników istnieje podobny mechanizm. Zgodnie z tą regulacją wymaga się od podmiotów zbiorowych by posiadały zinstytucjonalizowany system *compliance*, którego istnienie i odpowiednie wykorzystanie nawet po fakcie popełnienia przestępstwa może prowadzić do uwolnienia od odpowiedzialności (kwestia zwolnienia z odpowiedzialności podmiotów zbiorowych za przestępstwa pracowników została omówiona w części dotyczącej Criminal Compliance). To rozwiązanie prawne, choć dotyczyło odpowiedzialności podmiotów zbiorowych, stanowiło dla autora inspirację do zaproponowania podobnego instrumentu względem pracowników instytucji finansowych.

Problemem związanym z kwalifikacją prawną rekomendacji jest kwestia możliwości niezastosowania się do nich przez instytucje finansowe. Szczególnie interesująco zarysowywałaby się sytuacja, w której instytucja finansowa nie implementuje do swojego wewnętrznego regulaminu rekomendacji

[44] Krakowska szkoła prawa karnego uznaje, że do stwierdzenia określonego zachowania za przestępstwo w rozumieniu Kodeksu karnego należy je zakwalifikować jako czyn bezprawny, karalny, karygodny i zawiniony.

organu nadzorczego, a pomimo to jej pracownik postępuje zgodnie z takimi zaleceniami. Jeżeli przyjąć, że nie są one przepisami wiążącymi, wewnętrznymi aktami prawnymi, to instytucje finansowe mogą być wyposażone w mechanizm, który został wspomniany wyżej, czyli *comply or explain*. Mogą zatem odmówić zastosowania się do rekomendacji pod warunkiem, że przekonywująco uzasadnią swoją decyzję i wykażą, że nie stosując się, są w stanie osiągnąć założenia nadzorcze. Jeżeli nie będą w stanie tego uzasadnić albo odmówią, to mogą zostać umieszczone na publicznej liście (ang. *shame list*). Obecnie jednak w polskim porządku prawnym nie mogą one skorzystać z takiego mechanizmu z uwagi na kompetencję Komisji Nadzoru Finansowego do podjęcia administracyjnych środków represyjnych. Skłania to do stwierdzenia, że rekomendacjom bliżej jest do wewnętrznych źródeł prawa niż do *soft law*[45].

Należy zatem uznać, że polski rynek finansowy, który przecież jest sektorem gospodarki, podlegający niemalże zbalansowanym wpływom prawa prywatnego i publicznego, dla swojej stabilności wymaga doprecyzowania roli rekomendacji. Zaraz za nią powinien pójść instrument zachęcający do ich przestrzegania, zarówno przez instytucje finansowe, jak i ich pracowników, tak by ciężar implementacji instrukcji organu nadzorczego wiązał się z wymiernymi korzyściami. Takie instrumenty gwarancyjne pozwolą zarówno Komisji Nadzoru Finansowego, jak i samym instytucjom bankowym na lepszą kontrolę i przeciwdziałanie przestępczości.

Konstruowanie szczególnej komórki ds. odpowiedzialności podmiotów zbiorowych (Criminal Compliance).

Poniższa propozycja mechanizmu przeciwdziałania przestępczości pracowników instytucji finansowych i przeciwdziałania odpowiedzialności instytucji finansowych za takie czyny nie wymaga ingerencji w powszechny porządek prawny, jest ona bowiem rozwiązaniem, które może być pozostawione sferze rekomendacji organu nadzorczego bądź nawet wyłącznie wewnętrznym regulacjom instytucji finansowych.

[45] Por. https://piu.org.pl/public/upload/ibrowser/WU/WU1_2015/WU%201-2015%2009%20pabian%20wajda.pdf [dostęp: 8.12.2018].

Tezy:

1. Należy stworzyć w ramach struktury organizacyjnej instytucji finansowej nową komórkę ds. zgodności o szczególnej roli (Criminal Compliance). Jej zadania będą zorientowane wyłącznie na materię prawa karnego i będą miały dwojaki charakter – przeciwdziałanie przestępczości pracowników instytucji finansowych oraz przeciwdziałanie potencjalnej odpowiedzialności podmiotów zbiorowych w razie nieefektywnego lub nieskutecznego programu prewencyjnego.
2. Pierwszym zadaniem Criminal Compliance będzie przeciwdziałanie przestępczości pracowników instytucji finansowych. W drodze implementowania dobrych praktyk, szkoleń i nadzorowania operacji pracowników będą ograniczały prawdopodobieństwo wystąpienia działań przestępnych w organizacji.
3. Drugim zadaniem Criminal Compliance będzie nadzorowanie, by mechanizmy przeciwdziałania przestępczości pracowniczej spełniały prawne standardy. Osiągnięcie ich pozwoli na przypisanie odpowiedzialności karnej wyłącznie sprawcy przestępstwa, bez odpowiedzialności reprezentowanej przez niego instytucji finansowej. Jest to instrument subsydiarny do środków prewencji i będzie wykorzystany dopiero przy niepowodzeniu pierwszego zadania komórki ds. zgodności działań z prawem karnym.

Uzasadnienie:

Wewnętrzne procedury kontrolne, nazywane obecnie *compliance services*[46], to na ten moment coraz popularniejsze mechanizmy służące eliminowaniu nieprawidłowości w przedsiębiorstwach różnego rodzaju – szczególnie tych, które pełnią szczególną rolę społeczną i nie można ich jednoznacznie zakwalifikować do podmiotów, których działalność operacyjna regulowana jest wyłącznie przez przepisy prawa prywatnego. Do takich podmiotów można zaliczyć organizacje zajmujące się zarządzaniem danymi osobowymi, żywnością, lekami, ale też podmioty funkcjonujące w ramach rynku finansowego. Na

[46] Więcej o znaczeniu tego terminu i jego rozwoju w części 2 (*Grundlagen*), rozdziale *Compliance* autorstwa Ute Bottmanna [w:] *Kapitalmarktstrafrecht*, red. T. Park, Göttingen 2008.

tych ostatnich ciąży bowiem szczególna odpowiedzialność. Są dla gospodarki czymś w rodzaju układu krwionośnego dla organizmu. Pełnią rolę pośredników między posiadaczami środków pieniężnych i tymi, którzy są skłonni odpłatnie z nich korzystać.

Komórki ds. *compliance* z każdym rokiem stają się w Polsce coraz bardziej popularne. Popularyzacja tych rozwiązań prawnych, powstałych w latach 90. ubiegłego wieku w Stanach Zjednoczonych Ameryki Północnej[47], znacznie wzrosła po kryzysie gospodarczym 2007+, gdy uświadomiono sobie, że niektórzy pracownicy instytucji finansowych zrezygnowali ze swojej służebnej roli pośrednika finansowego na rzecz partykularnych interesów polegających na uzyskiwaniu jak największej prowizji sprzedażowej. Wtedy to uświadomiono sobie, że instytucje finansowe, tak jak służby państwowe (np. policja), dla zapewnienia wewnętrznego porządku i przestrzegania przepisów muszą mieć wewnętrzne komórki zajmujące się kontrolą przestrzegania reguł działalności na rynku finansowym.

Obecnie w instytucjach finansowych działających na terenie Rzeczypospolitej Polskiej niemalże wszystkie podmioty w swojej strukturze organizacyjnej posiadają komórkę ds. *compliance*. Są powoływane do życia w celu badania, czy organy zarządcze w swoim działaniu wdrażają należyte praktyki oraz czy przepisy związane z prowadzeniem działalności gospodarczej są przestrzegane przez nadzorowaną z zewnątrz instytucję. Można jednak z grupy takich podmiotów nadzorczych wyodrębnić podmiot o szczególnym charakterze (Criminal Compliance), którego zadaniem będzie prowadzenie czynności nadzorczych służących prowadzeniu przedsiębiorstwa zgodnie z przepisami prawa karnego[48]. Z jednej strony ta jednostka ma przeciwdziałać przestępstwom pracowników instytucji finansowej, a z drugiej ma dążyć do ograniczenia odpowiedzialności przedsiębiorstwa w razie popełnienia przestępstwa przez pracowników. Zatem, nawet jeśli komórce ds. Criminal Compliance nie uda się przeciwdziałać przestępstwom pracowniczym, to dzięki prowadzeniu przedsiębiorstwa zgodnie z wszelkimi normami prawnymi, do odpowiedzialności karnej będzie można pociągnąć wyłącznie bezpośredniego sprawcę

[47] Protoplastą *compliance* był model kontroli wewnętrznej COSO.

[48] Na potrzebę takiego wyodrębnienia zwraca się uwagę w niemieckim piśmiennictwie, patrz: T. Rotsch, *Criminal Compliance*, „Zeitschrift für Internationale Strafrechtsdogmatik" 2010, no. 10.

przestępstwa, co z pewnością wpłynie na jego potencjalną motywację do popełnienia przestępstwa. Nikt bowiem nie chciałby być przedstawiony jako „kozioł ofiarny", szczególnie gdy przestępstwo, które popełnił, miało przynieść korzyść wyłącznie organizacji, gdzie pracuje.

Jeżeli chodzi o organizację strukturalną pierwszego zadania, to bardzo pomocne wydają się materiały rekomendacyjne dla prokuratorów (tzw. memorandum Thompsona[49]), które powstały na kanwie sprawy Enrona, czyli amerykańskiej spółki paliwowej, w której zdiagnozowano szereg przestępstw pracowniczych, a także wytyczne dla sędziów wydziałów kryminalnych sporządzone przez niezależną agencję United States Sentencing Commission[50].

W tym ostatnim dokumencie, w części dotyczącej dyrektywy wymiaru kary, wyliczono 7 przesłanek efektywnego systemu prewencji kryminalnej (sam fakt popełnienia przestępstwa przez pracownika nie oznacza, że system prewencyjny jest nieefektywny) wewnątrz struktury organizacyjnej przedsiębiorstwa. Są nimi:

– **wyodrębnienie wewnątrz przedsiębiorstwa komórki Criminal Compliance**

Taka odrębność organizacyjna podmiotu nadzorczego pozwala na zwiększenie efektywności podejmowanych działań. Po pierwsze, pozostawianie obowiązków nadzorczych zarządowi godzi w rolę tego podmiotu w ramach przedsiębiorstwa. Wszak głównym obszarem jego obowiązków jest działalność operacyjna, a działania kontrolne wymagają zupełnie innych metodyk.

– **nadzór prowadzony przez tę szczególną jednostkę powinien być wykonywany przez pracowników wysokiego szczebla, tak by był on w pełni świadomy i zrozumiały (takie procedury wymagają całościowej wiedzy o modelu biznesowym, charakterze operacji wykonywanych przez pracowników oraz przede wszystkim kompetencji nadzorczych i niezależności)**

---

[49] https://www.americanbar.org/content/dam/aba/migrated/poladv/priorities/privilegewaiver/2003jan20_privwaiv_dojthomp.authcheckdam.pdf [dostęp: 5.12.2018].

[50] A. Krawczyk, A. Gisman, *Criminal compliance jako środek zapobiegania odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary*, „Monitor Prawa Handlowego" 2015, nr 1.

– zatrudnienie w wydziale zajmującym się działalnością organizacyjną osób, które będą zdawały sprawozdania bezpośrednio do personelu wyższego szczebla odpowiedzialnego za przeprowadzenie nadzoru

Zapewnienie bezpośredniego i szybkiego kanału wymiany informacji jest kluczowe dla przeciwdziałania przestępczości pracowników. Pozwala bowiem na zdecentralizowaną kontrolę wewnątrz określonych departamentów i zbieranie pozyskanych informacji oraz ich przetwarzanie na wyższym szczeblu[51]. Takie podejście jest nie tylko bardziej efektywne, ale pozwala też na kompleksową kontrolę krzyżową transakcji.

– szkolenie personelu, który zajmuje się nadzorem zgodności, ale też pozostałych pracowników przedsiębiorstwa w kwestii regulacji prawnych oraz etycznych standardów i procedur

Analiza prawna zarządzania operacjami w sektorze finansowym, kreatywności i innowacyjności w zarządzaniu, nowych technologii integrujących informacje w zarządzaniu operacjami oraz dostępności na świecie rozwiązań problemów przestępczości w sektorze finansowym jest nieodłącznym elementem procedur *compliance*. Bez cyklicznego edukowania personelu odpowiednich wzorców zachowań nie da się zredukować poziomu przestępczości wewnątrz struktury organizacyjnej. Z jednej strony muszą być oni świadomi, jakie czynności operacyjne są dozwolone, a jakie zakazane. Z drugiej strony taka edukacja pozwala też innym pracownikom na kontrolowanie działań swoich koleżanek i kolegów (pozycja prawna sygnalistów została opisana w innej części opracowania).

– okresowe monitorowanie i badanie efektywności programu nadzorczego

Ciągłe badanie skuteczności programu w połączeniu z jego udoskonalaniem jest niezbędnym elementem dobrych procedur nadzorczych. Jest to szczególnie ważne w dobie szybkiego postępu technologicznego, który z każdym dniem może przyjąć jeszcze bardziej wyszukane metody popełniania przestępstw.

---

[51] Jest to połączenie modelu centralnego i rozproszonego. Uznaje się, że taki właśnie wymagany jest od polskich instytucji finansowych (patrz: Ł. Cichy, *Funkcja compliance w bankach*, Warszawa 2015, s. 10.)

– zbudowanie i upowszechnianie modelu anonimowego i poufnego raportowania o nieprawidłowościach występujących w przedsiębiorstwie[52] (ta kwestia będzie przedmiotem odrębnej części niniejszego opracowania)

– konsekwencja we wdrażaniu programu, włącznie z bezwzględnym dyscyplinowaniem osób nieprzestrzegających zasad i procedur

Obiektywne podejście do procedur kontrolnych jest kluczowe dla zaszczepienia w pracownikach odpowiedniej mentalności dotyczącej kultury korporacyjnej. Różne traktowanie zachowań naruszających ogólnie przyjęte normy działa demotywująco na pracowników i ogranicza ich skłonność do współpracowania z komórkami do spraw zgodności w celu skutecznego nadzoru instytucji finansowych.

– w razie zaistnienia działania przestępnego dalsze przeciwdziałanie przestępczości (udoskonalone przez wewnętrzną analizę przyczyn nieskutecznej prewencji) połączone z adekwatną reakcją

Wydaje się, że wskazane wyżej kierunki działania będą mogły mieć zastosowanie do Criminal Compliance wewnątrz instytucji finansowej. Choć w porównaniu do przedsiębiorców z innych gałęzi gospodarki, systemy *compliance* są w prywatnym sektorze finansowym znacznie bardziej popularne, to powołanie do życia szczególnego podmiotu zajmującego się wyłącznie problemem przestępczości wśród pracowników wydaje się uzasadnione. Szczególnie że znacznie większa część przestępstw pracowników instytucji finansowych jest dokonywana przez personel niższego szczebla (są to zwykle przestępstwa korupcyjne, księgowe czy informatyczne; przestępstwa pracowników wyższego szczebla występują znacznie rzadziej, ale dokonywane są na większą skalę).

Jeśli zaś chodzi o odpowiedzialność instytucji finansowych za przestępne czyny pracowników (w razie nieskutecznego systemu prewencyjnego), zatem o drugie zadanie, jakie stoi przed komórkami ds. Criminal Compliance, to w polskim porządku prawnym jest przedmiot regulacji ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny

[52] *Ibidem*, s. 22.

zabronione pod groźbą kary[53]. Tytułowym podmiotem zbiorowym jest zgodnie z tą ustawą osoba prawna, ale też jednostka organizacyjna nieposiadająca osobowości prawnej, której ustawa przyznaje zdolność prawną, spółka handlowa z udziałem Skarbu Państwa, spółka kapitałowa w organizacji, podmiot w stanie likwidacji oraz przedsiębiorca niebędący osobą fizyczną. Wydaje się jednak, że wszystkie instytucje finansowe mogą być zakwalifikowane do tej pierwszej kategorii.

Przesłankami determinującymi możliwość przypisania odpowiedzialności instytucji finansowej za przestępstwo popełnione przez jej pracowników są:

a) stwierdzenie w drodze prawomocnego orzeczenia karnego stwierdzającego winę sprawcy, popełnienia przez osoby reprezentujące instytucję finansową przestępstwa albo przestępstwa skarbowego (wpływ przestrzegania rekomendacji organu nadzorczego przez pracowników na bezprawność czynu została omówiona w części dotyczącej zmian statusu prawnego rekomendacji Komisji Nadzoru Finansowego),
b) brak należytej staranności instytucji finansowej w wyborze osoby reprezentującej ją lub brak należytego nadzoru nad tą osobą („quasi-winа w nadzorze") lub nieprawidłowa organizacja działalności instytucji, która nie pozwoliła na przeciwdziałanie popełnieniu przestępstwa („quasi-wina w organizacji"),
c) przysporzenie na rzecz instytucji korzyści finansowej albo taka możliwość.

Z uwagi na przedmiot opracowania należy się skupić na drugiej przesłance, która dotyczy mechanizmów nadzorczych nad pracownikami, a szczególnie na dwu ostatnich postaciach quasi-winy. Należy zwrócić uwagę, że przypisanie odpowiedzialności instytucji finansowej nie jest tutaj oparte na winie w znaczeniu prawa karnego, ale raczej na czymś w rodzaju quasi-winy[54], bo tej pierwszej nie można przecież przypisać podmiotom innym niż osoby fizyczne. Można tutaj jednak odnaleźć charakterystyczny dla prawa karnego

[53] Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz.U. 2002 Nr 197, poz. 1661).

[54] Na bliską naturę tej winy z winą w rozumieniu prawa cywilnego zwraca uwagę: D. Habrat, *Ustawa o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary. Komentarz*, *Komentarz do art. 5*, Warszawa 2014.

ciężar dowodu na oskarżycielu połączony z wymogiem wykazania związku przyczynowego między popełnieniem przestępstwa a wadliwym procesem nadzorczym przedsiębiorstwa[55].

Wracając do wpływu Criminal Compliance na odpowiedzialność instytucji finansowych za przestępstwa popełniane przez ich pracowników, można stwierdzić, że system prewencyjny zgodny z zaleceniami wskazanymi w części dotyczącej pierwszego zadania komórki ds. zgodności działań instytucji finansowej z prawem karnym walnie obniża prawdopodobieństwo ukarania takich przedsiębiorstw. Powołanie do życia szczególnej jednostki, której zadaniem jest przeciwdziałanie określonym zachowaniom pracowników instytucji finansowej, świadczy o profesjonalnym podejściu do procedur nadzorczych. Trudno bowiem wykazać winę w organizacji, jeśli podmiot wdrożył skutecznie mechanizmy wewnętrznego nadzoru. Podobny problem z przypisaniem odpowiedzialności będzie istniał przy należytym egzekwowaniu przez jednostki ds. zgodności procedur nadzoru[56].

Jeżeli chodzi o efektywne wdrożenie mechanizmów pozwalających na realizowanie drugiego zadania stojącego przez Criminal Compliance, to najpierw należy zdiagnozować, jakie ryzyka w perspektywie karnej czyhają na pracowników instytucji finansowych. I tutaj trudno o ogólną odpowiedź, bo jest to materia uzależniona od specyfiki działalności operacyjnej konkretnego podmiotu. Pomocnym instrumentem w trakcie takiego audytu będzie analiza dotychczasowych przypadków popełnienia przestępstw przez pracowników. Na podstawie wniosków badawczych można zarysowywać kierunki pożądanych działań, które powinny być znane wszystkim pracownikom. Zapoznanie wszystkich z ustalonymi standardami powinno być też wsparte odpowiednimi szkoleniami, szczególnie dla organów wyższego szczebla, które są odpowiedzialne za procedury nadzorcze. Jeżeli zaś chodzi o ścisłe procedury przeciwdziałania przestępczości, to zapewnienie pracownikom możliwości anonimowego zgłaszania nieprawidłowości w połączeniu z potencjalnymi dochodzeniami prowadzonymi przez pracowników komórki ds. Criminal Compliance pozwoli na uświadomienie pracownikom,

[55] M. Filar, *Odpowiedzialność podmiotów zbiorowych za czyny zabronione pod groźbą kary*, [w:] *System prawa karnego*, t. 1, red. A. Marek, Warszawa 2010, s. 432.

[56] Szerzej: A. Krawczyk, A. Gisman, *op. cit.*

że zachowania przestępne lub niezgodne z ustalonymi procedurami będą niezwłocznie odnotowywane, a niesubordynacja – niezwłocznie karana. Bowiem to nieuchronność kary, a nie jej dolegliwość jest najsilniejszym bodźcem przeciwdziałającym nagannym zachowaniom.

Należy więc podkreślić, że komórki ds. zgodności z prawem karnym nie tylko nadzorują działania pracowników w celu redukcji przestępczości, ale też są odpowiedzialne za uświadamianie w kwestii regulacji prawnokarnych. Ich zadania informacyjne i edukacyjne pełnią też rolę wychowawczą, zbliżoną do regulacji prawa karnego. Choć takie dodatkowe komórki organizacyjne wymagają dodatkowych nakładów poniesionych przez instytucje finansowe, to w dłuższej perspektywie są niezwykle korzystne, gdyż pozwalają na ograniczenie przestępczości, a nawet całkowite zniwelowanie przestępczości wśród pracowników. Jeżeli nawet osiągnięcie tego celu w całości okaże się nieosiągalne, to wdrożenie odpowiednich i efektywnych procedur pozwoli na uniknięcie potencjalnej odpowiedzialności za przestępstwa pracowników. Wewnętrzne dochodzenia są tutaj szczególnie ważne, gdyż dostarczają niezbędnego materiału dowodowego w razie podjęcia przez oskarżyciela działań zmierzających do ukarania instytucji finansowej. Ich zebranie pozwala w łatwiejszy sposób udowodnić, że podjęto niezbędne działania do sprawowania nadzoru z należytą starannością.

Pozostawienie kwestii zorganizowania Criminal Compliance bez ingerencji w drodze uchwalenia odgórnych przepisów powszechnie obowiązujących ma na celu podkreślenie fakultatywnego charakteru tych regulacji oraz zwrócenie uwagi na wielowymiarowość organizacji takiego systemu. Nadmierne usztywnienie procedur nadzorczych byłoby niekorzystne dla samych podmiotów implementujących ten aparat. Niezwykle trudno byłoby na poziomie ustawodawczym zaproponować instytucjom finansowym, które przecież prowadzą swoją działalność operacyjną w zróżnicowany sposób, spójnego systemu, który mógłby być przedmiotem bezpośredniej implementacji. Z tych powodów w tej części opracowania zostały wskazane tylko pewne kierunki i założenia organizacyjne komórki ds. zgodności działań z prawem karnym[57]. Podlegają one oczywiście ciągłemu uaktualnieniu z powodu ciągłego postępu

[57] Dla sektora finansowego wymogi dotyczące komórek ds. *compliance* mają bardziej precyzyjny charakter. Wynika to z faktu szczególnej roli tych podmiotów w gospodarce.

technologicznego, który jest zagrożeniem, ale też szansą dla prywatnego sektora finansowego. Dla zwiększenia skuteczności procesów nadzorczych należałoby rozważyć wprowadzenie zintegrowanego systemu dla wszystkich podmiotów, tak by mogły się one skutecznie wymieniać się pozyskanymi informacjami i doświadczeniem.

2.3. Regulacja pozycji prawnej sygnalistów

Charakter zmian: uchwalenie nowego aktu prawnego dotyczącego pozycji prawnej sygnalistów w instytucjach finansowych
Obszar zmian: nowa ustawa, Kodeks karny, prawo bankowe, Kodeks postępowania karnego, ustawa o przeciwdziałaniu praniu brudnych pieniędzy i finansowaniu terroryzmu

Tezy:

1. Należy zbudować wewnętrzny i zewnętrzny zinstytucjonalizowany system pozwalający na działalność sygnalistów w instytucjach finansowych, służący do zgłaszania jak najszerszego katalogu nieprawidłowości czy przestępstw. Stworzenie takich mechanizmów wyłącznie dla przestępstw prania pieniędzy i finansowania terroryzmu nie jest wystarczające dla skutecznego przeciwdziałania przestępczości pracowników instytucji finansowych.
2. Osoba decydująca się na bycie sygnalistą musi mieć zagwarantowaną ochronę prawną, zarówno przy procedurze wewnętrznej, jak i zewnętrznej. Konstrukcja anonimowego informowania nie stanowi wystarczającej gwarancji prawnej dla sygnalisty, gdyż często można drogą indukcji zidentyfikować źródło pochodzenia informacji[58]. Należy wdrożyć dodatkowe gwarancje (zakaz zwolnienia, preferencyjne warunki przywrócenia do pracy czy dodatkowe uprzywilejowanie w ewentualnym sporze z pracodawcą).

[58] Więcej: A. Kobylińska, M. Folta, *Sygnaliści – ludzie, którzy nie potrafią milczeć. Doświadczenia osób ujawniających nieprawidłowości w instytucjach i firmach w Polsce*, Warszawa 2015, s. 33 i n.

3. Osoba korzystająca z mechanizmu powinna mieć w tym procederze „czyste ręce". W razie wykazania umyślnego udziału w przestępstwie albo innym nagannym społecznie zachowaniu, które jest przedmiotem zgłoszenia, powinna być współoskarżonym zarzucanych innym czynów. Okoliczność zaprzestania partycypacji w przestępstwie będzie miała wpływ na ewentualną karalność czynu (złagodzenie kary albo nawet uniknięcie odpowiedzialności przez sprawcę, zarówno przy czynnym żalu skutecznym, jak i nieskutecznym).
4. Należy rozważyć dopuszczalność gratyfikowania osób, które zdecydowały się na poinformowanie o nieprawidłowościach w ramach instytucji finansowych (szczególnie przy ewentualnym braku współdziałania przestępczego, gdzie nie występuje gratyfikacja sygnalizmu w postaci złagodzonej albo zniesionej odpowiedzialności karnej wskutek czynnego żalu).

Uzasadnienie:

Analiza prawna w kontekście kultury organizacyjnej wspierającej postawy praworządności, tworzenia strategicznych scenariuszy na przyszłość, innowacyjnych strategii rozwoju gospodarczego oraz przygotowania na nowe rodzaje przestępstw w przyszłości powinna odnosić się do udziału samych pracowników w wykrywaniu i reagowaniu na zachowania naganne społecznie. W działalności organizacji finansowych, których model biznesowy oparty jest w założeniu na służbie na rzecz klientów i silnie akcentowanej dobrej wierze w stosunku zobowiązaniowym, ostatnimi czasy można było dostrzec zjawiska będące odchyleniem od założeń. Kryzys roku 2007 i lat następnych uzmysłowił badaczom, że pracownicy instytucji finansowych w pogoni za prowizjami i rosnącymi wymaganiami sprzedażowymi zatracili się w relacji prawnej ze swoimi klientami i osadzili ją nie na fundamencie dobrej wiary, a na mechanizmie *moral hazard*. Przesuwając niemal całe ryzyko na klientów banku (ryzyko inwestycyjne) i podatników (ryzyko systemowe; ta grupa musiała zapłacić za liczne *bail-outy* instytucji finansowych), nie ponosili konsekwencji swoich działań, podejmując mniej ostrożne decyzje, które równocześnie gwarantowały zyski prowizyjne. Ta cezura sprawiła, że regulacje prawne dotyczące instytucji finansowych wymagały gruntownych zmian.

Jednym z mechanizmów, który ma zapewnić kontrolę nad legalnością operacji pracowników instytucji finansowych jest instytucjonalizacja pozycji prawnej sygnalisty (ang. *whistleblower*), czyli osoby, która informuje o nieprawidłowościach występujących w ramach podmiotu, dla którego pracuje, i stanowiących zagrożenie dla interesu publicznego[59]. I choć takie działanie budzi czasem etyczne wątpliwości (negatywne skojarzenie z donosicielstwem), to jest bardzo skutecznym sposobem na odkrywanie nieprawidłowości w ramach organizacji. Warto też wspomnieć, że kluczowe międzynarodowe akty prawne zobowiązują polskiego ustawodawcę do wprowadzenia bądź rozważenia regulacji dotyczących pozycji prawnej sygnalistów. Pierwszym z nich jest Cywilnoprawna konwencja o korupcji[60], która w art. 9 stanowi, co następuje:

> Art. 9. Ochrona pracowników
> Każda Strona zapewni w swoim prawie wewnętrznym odpowiednią ochronę przed wszelkimi nieuzasadnionymi sankcjami wobec pracowników, którzy mając uzasadnione podstawy do podejrzewania, że doszło do korupcji, zgłaszają w dobrej wierze swoje podejrzenia odpowiednim osobom lub władzom.

Drugi akt prawny obligujący do rozważenia to Konwencja Organizacji Narodów Zjednoczonych przeciwko korupcji[61], która w art. 33 stanowi:

> Każde z Państw Stron rozważy włączenie do swego wewnętrznego systemu prawnego stosownych środków zapewniających ochronę przed każdym niesprawiedliwym traktowaniem osoby, która zgłasza w dobrej wierze i na racjonalnych podstawach właściwemu organowi wszelkie zdarzenia związane z przestępstwami określonymi zgodnie z niniejszą Konwencją.

W polskim porządku prawnym można odnaleźć dwa główne akty prawne, które odnoszą się do pozycji prawnej sygnalisty w instytucji finansowej. Pierwszy z nich to ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe,

---

[59] Więcej na: https://www.iaca.int/images/Research/Research_paper_05_Ruggero_Scaturro_final.pdf [dostęp: 8.12.2018].

[60] Cywilnoprawna konwencja o korupcji (Dz.U. 2004 Nr 244, poz. 2443).

[61] Konwencja Narodów Zjednoczonych Przeciwko Korupcji przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych z dnia 31 października 2003 r. (Dz.U. 2007 Nr 84, poz. 563).

do której wskutek uchwalenia rozporządzenia Parlamentu Europejskiej i Rady nr 596/2014 weszły przepisy dotyczące obowiązku stworzenia w banku systemu zarządzania, obejmującym także procedury anonimowego zgłaszania wskazanemu członkowi zarządu albo radzie nadzorczej banku naruszeń prawa oraz obowiązujących w banku procedur i standardów etycznych.

Nowelizacja gwarantuje sygnalistom minimalny standard ochrony, zobowiązując bank do ochrony przed dyskryminacją czy innymi działaniami o charakterze represyjnym. W ustawie znajduje się delegacja, która pozostawia ministrowi właściwemu ds. instytucji finansowych doprecyzowanie wspomnianych oddolnych procedur nadzorczych. Minister w drodze rozporządzenia zobowiązał instytucje finansowe do sporządzenia katalogu procedur, w drodze których pracownik może zgłaszać fakt powstania naruszenia[62]. Ponadto, zobligował je też do zapewnienia sygnalistom odpowiednich gwarancji i powołania struktur zajmujących się odbieraniem takich zgłoszeń. W kwestii tej regulacji należy zwrócić uwagę na dwie kwestie.

Po pierwsze, regulacja ta odnosi się wyłącznie do wewnętrznych gwarancji i do wewnętrznego procesu sygnalizowania nieprawidłowości. Nie sposób odnaleźć w niej spójny mechanizm informowania i reagowania organów państwowych, zewnętrznych wobec podmiotu, w którym doszło do powstania nieprawidłowości. Takie regulacje zdają się tylko cząstkowe i właściwe nie dla naruszeń prawa powszechnie obowiązującego, lecz wewnętrznych praktyk i procedur banku.

Z drugiej strony, negatywnie należy ocenić obciążenie obowiązkiem przyjmowania zgłoszeń wyłącznie przez członków zarządu, bądź przez radę nadzorczą w razie, gdy naruszenia są spowodowane przez członka zarządu. Obciążanie tych podmiotów szeregiem obowiązków nadzorczych nie może być efektywną decyzją, gdyż zbudowanie struktury do sygnalizowania nieprawidłowości nie polega wyłącznie na stworzeniu anonimowego kanału informacyjnego i przyjmowaniu ewentualnych zgłoszeń. Nieodzownym elementem tej struktury jest proces informacyjny pracowników, którzy

[62] Rozporządzenie Ministra Rozwoju i Finansów w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (Dz.U. z 2017 r., poz. 637).

bez niego nie będą świadomi, czy rzeczywiście wewnątrz organizacji dochodzi do nieprawidłowości.

Drugim aktem prawnym, który zawiera przepisy dotyczące pozycji prawnej sygnalistów, jest ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[63]. Można w niej znaleźć przepisy zobowiązujące instytucje finansowe do opracowania i wdrożenia procedury anonimowego zgłaszania przez pracowników albo inne osoby reprezentujące instytucje albo wykonywujące na jej rzecz czynności, potencjalnych naruszeń przepisów prawnych dotyczących prania pieniędzy albo finansowania terroryzmu. Ustawodawca pozostawił instytucjom zobowiązanym zbudowanie struktury organizacyjnej. Wskazał, że muszą one w swojej organizacji określić:

1) osobę odpowiedzialną za odbieranie zgłoszeń;
2) sposób odbierania zgłoszeń;
3) sposób ochrony pracownika dokonującego zgłoszenia, zapewniający co najmniej ochronę przed działaniami o charakterze represyjnym, dyskryminacją lub innymi rodzajami niesprawiedliwego traktowania;
4) sposób ochrony danych osobowych pracownika dokonującego zgłoszenia oraz osoby, której zarzuca się dokonanie naruszenia, zgodnie z przepisami o ochronie danych osobowych;
5) zasady zachowania poufności w przypadku ujawnienia tożsamości osób, o których mowa w pkt 4, lub gdy ich tożsamość jest możliwa do ustalenia;
6) rodzaj i charakter działań następczych podejmowanych po odebraniu zgłoszenia;
7) termin usunięcia przez instytucje obowiązane danych osobowych zawartych w zgłoszeniach.

Ponadto ustawodawca przewidział obowiązek przekazywania Generalnemu Inspektorowi Informacji Finansowej sprawozdań dotyczących wszelkich informacji o podejrzeniach prania pieniędzy lub finansowania terroryzmu oraz o przeprowadzonych analizach dotyczących tych przestępstw.

Oceniając przedstawione wyżej regulacje, należy zwrócić uwagę, że są one wyłącznie fragmentaryczne. Pierwszy akt prawny w gruncie rzeczy zobowiązuje instytucje finansowe do zbudowania wewnętrznej struktury

[63] Dz.U. 2018 r., poz. 723.

informowania o nieprawidłowościach. Wydaje się jednak, że działalność sygnalisty, która ma ogromny wpływ na interes publiczny, została tutaj zlekceważona. Prawodawca przeniósł bowiem cały ciężar regulacyjny na barki instytucji finansowych, które z racji skali swojej działalności mogą zbudować wyłącznie wewnętrzne struktury mechanizmu demaskowania nieprawidłowości.

W części o pozycji prawnej należy jeszcze zwrócić uwagę, że polski porządek prawny znajduje inne odniesienia do sygnalizmu. Mowa tutaj o przepisach, które przewidują obowiązki sygnalizacyjne. Art. 304 § 1 k.p.k. nakłada na każdego, kto dowiedział się o popełnieniu przestępstwa ściganego z urzędu, społeczny obowiązek zawiadomienia o tym prokuratora lub Policji. Podobny obowiązek, choć jego adresatem są wyłącznie pracownicy, nakładany jest w ramach dbania o dobro zakładu pracy. Na podstawie art. 100 § 2 pkt 4 k.p. każdy, kto dostrzega nieprawidłowości w funkcjonowaniu swojego zakładu pracy, zobowiązany jest do zasygnalizowania takiego faktu.

Regulację dotyczącą pozycji prawnej sygnalistów i ich ochrony należy rozpocząć od zdefiniowania, kto rzeczywiście może nim być. Wydaje się, że może to być zarówno osoba zatrudniona w instytucji finansowej, reprezentująca ją, ale też pozostająca w faktycznym stosunku podległości. Ponadto, ochroną powinni zostać objęci zarówno ci, którzy zgłaszają nieprawidłowości, jak i wszyscy, którzy przyczynili się do takiego zgłoszenia.

Warunkiem koniecznym do zagwarantowania takiej osobie ochrony prawnej są jej dobre intencje w zgłaszaniu nieprawidłowości oraz prawdziwość przekazanych informacji[64]. Rzecz jasna nie można wymagać od takiego podmiotu kompleksowej analizy. Badanie prawdziwości przekazanych informacji jest zorientowane na przekazane dokumenty, a nie na ich interpretację. Ta pozostaje w gestii odpowiednich komórek nadzorczych. Co do wpływu ewentualnego współuczestnictwa pracownika instytucji finansowej, którego zaniechał i następnie stał się sygnalistą, problem ten zostanie omówiony w późniejszej części opracowania.

[64] Definiując rolę sygnalisty, mocno podkreśla się jego dobrą wiarę przy zgłaszaniu nieprawidłowości – patrz https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/guidance-for-whistleblowers/ [dostęp 8.12.2018].

System informowania o nieprawidłowościach w instytucjach finansowych należy podzielić na dwa etapy. Pierwszy z nich to etap wewnętrzny[65], który warunkuje przejście do etapu zewnętrznego. Taka hierarchia ma swoje źródło w obowiązku lojalności pracownika względem pracodawcy, które mają swoje źródło w zasadach współżycia społecznego oraz przepisach Kodeksu pracy. Skorzystanie od razu z zewnętrznego systemu informowania powinno skutkować brakiem ustawowej ochrony sygnalisty. Wewnętrzny system informowania o nieprawidłowościach powinien przede wszystkim wiązać się z:

1) uprzednim szkoleniem pracowników co do okoliczności, które należy uznać za niepokojące,
2) uprzednim szkoleniem pracowników co do mechanizmu działania systemu,
3) zagwarantowaniem poufności informacji oraz tożsamości sygnalisty,
4) wskazaniem osoby odpowiedzialnej za przyjmowanie zgłoszeń (powinna to być osoba zatrudniona w ramach odrębnej jednostki nadzorczej wewnątrz struktury organizacyjnej – np. w ramach Criminal Compliance),
5) zagwarantowaniem sygnaliście ochrony przed odwetem ze strony osób, których zawiadomienie dotyczyło,
6) dogłębnym i rzetelnym badaniem prawdziwości wszystkich przekazanych informacji,
7) uprzednim określeniem środków i sposobów działania po uzyskaniu zawiadomienia,
8) udokumentowaniem całej procedury nadzorczej od momentu zasygnalizowania problemu do jego rozwiązania,
9) umożliwieniem sygnaliście dostępu do dokumentacji dotyczącej procedury nadzorczej.

Jeżeli chodzi zaś o samą procedurę reagowania na informacje, to należy podkreślić, że powinna być ona możliwie jak najszybsza. Zgodnie z dylematem *Quis custodiet ipsos custodes* organom nadzorczym powinien być dany określony czas na podjęcie procedur nadzorczych, z naruszeniem którego będą wiązały się określone skutki zarówno dla sygnalisty, jak i całej procedury

[65] Więcej: J. Taylor, *Internal Whistleblowing in the Public Service. A Matter of Trust*, „Public Administration Review" 2018, vol. 78, issue 5, s. 717–726.

nadzorczej. Można przyjąć, że naruszenie siedmiodniowego terminu na wszczęcie postępowania powinno skutkować dopuszczalnością przekazania informacji przez sygnalistę podmiotom zewnętrznym.

Drugi etap procedury sygnalizowania nieprawidłowości w ramach instytucji finansowych będzie wiązał się z udziałem podmiotów zewnętrznych w trybie zgłaszania nieprawidłowości[66]. Ten subsydiarny instrument będzie miał najczęściej zastosowanie w razie popełnienia przestępstwa przez pracownika instytucji finansowej. Można więc powiedzieć, że będzie obecny tam, gdzie wewnętrzne mechanizmy nie będą skuteczne bądź gdzie interwencja państwa jest niezbędna. Będzie to zatem informowanie państwowych organów ścigania o możliwości popełnienia przestępstwa (w razie wszczęcia postępowania rozpoznawczego przepisami właściwymi będą przepisy Kodeksu postępowania karnego) bądź informowanie opinii publicznej za pośrednictwem mediów o nieprawidłowościach w praktykach realizowanych w ramach instytucji finansowej. W przypadku wszczęcia śledztwa, rzecz jasna, wszelkie materiały, które udało się zgromadzić wewnętrznym komórkom nadzorczym, będą przekazane prokuratorowi. Będzie to też probierzem potencjalnej odpowiedzialności podmiotu zbiorowego za przestępstwo popełnione przez jego pracownika czy reprezentanta, w razie niezagwarantowania odpowiedniego nadzoru czy niezbudowania odpowiedniej struktury organizacyjnej. Zewnętrzne ujawnienie nieprawidłowości powinno się też wiązać z podtrzymaniem wewnętrznych gwarancji dla sygnalisty. Przejście do drugiego etapu procedury nie może pozbawiać go należytej ochrony.

Gwarancje prawne zapewnione sygnaliście powinny być wielowymiarowe. Przede wszystkim powinien on mieć zapewnioną pełną ochronę swojej tożsamości. Jej ewentualne ujawnienie nie może nastąpić bez zgody osoby zainteresowanej. Ponadto, powinien być objęty szczególną ochroną przed retorsjami pochodzącymi od pracodawcy polegającymi na:

1) wypowiedzeniu umowy o pracę przez pracodawcę,
2) obniżeniu świadczenia, do wykonania którego jest zobowiązany pracodawca,

[66] R. Bosua, S. Milton, S. Dreyfus, R. Lederman, *Going Public. Researching External Whistleblowing in a New Media Age*, [w:] *International Handbook on Whistleblowing Research*, red. A.J. Brown, D. Lewis, W. Vandekerckhove, Cheltenham–Northampton 2014, s. 250–272.

3) zmianie obowiązków pracownika czy miejsca wykonywania pracy,
4) wymierzaniu kar dyscyplinarnych,
5) nierównym czy niesprawiedliwym traktowaniu.

Objęcie taką ochroną powinno trwać znacznie dłużej niż postępowanie dyscyplinarne, a w ewentualnych sporach sądowych to pracodawca powinien udowodnić, że podjęte przez niego środki nie korespondują z ujawnieniem przez pracownika nieprawidłowości wewnątrz przedsiębiorstwa. Z uwagi na ujawnianie informacji o szczególnej wadze dla interesu społecznego należałoby też objąć takie osoby pełną i specjalistyczną opieką prawną, nie tylko dla okazania wsparcia po postępowaniu nadzorczym, ale też dla zapewnienia osobom obawiającym się ujawnienia nieprawidłowości, że nie zostaną pozostawione samym sobie.

Kwestia ewentualnej odpowiedzialności karnej sygnalisty może mieć różne źródła. Pierwsze z nich może wiązać się z ewentualnym współsprawstwem sygnalisty w przestępstwie, którego zaistnienie jest przez niego ujawniane. Takie zachowanie można zakwalifikować jako czynny żal przy współdziałaniu przestępczym[67]. W zależności od efektu działań przestępczych może on przyjąć postać czynnego żalu skutecznego i czynnego żalu bezskutecznego.

Ten pierwszy polega na tym, że sprawca dobrowolnie zapobiegł dokonaniu czynu zabronionego. Efektem skutecznego odstąpienia od działania i przeciwdziałania jest niepodleganie karze przez współsprawcę.

Ten drugi zaś wiąże się z dobrowolnymi staraniami, które ostatecznie nie doprowadziły do zapobieżenia dokonaniu czynu zabronionego. Starania te muszą być rzeczywiste, a nie pozorne dla potencjalnego uniknięcia odpowiedzialności karnej. Bezskuteczność przeciwdziałania nie pozwala na uniknięcie odpowiedzialności karnej, lecz umożliwia złagodzenie ewentualnej kary za popełnienie przestępstwa. Kwestia odpowiedzialności karnej sygnalisty w razie współsprawstwa jest niezwykle istotna dla przeciwdziałania wykorzystywaniu tej kategorii prawnej dla partykularnych interesów. Z pewnością nie

[67] Z czynnego żalu może skorzystać tylko ten, który dobrowolnie zapobiegł dokonaniu czynu zabronionego, patrz: W. Wróbel, A. Zoll, *Polskie prawo karne. Część ogólna*, Kraków 2014, s. 270.

można zatem jednoznacznie powiedzieć, że status sygnalisty bezwzględnie wyłącza potencjalną odpowiedzialność karną.

W tym miejscu należy jeszcze rozważyć etyczną dopuszczalność systemu motywacyjnego sygnalisty[68]. Zagraniczne porządki prawne, na przykład w Stanach Zjednoczonych Ameryki Północnej, stanowe regulacje przewidują gratyfikacje dla osób, które ujawniły przestępstwo z wykorzystaniem mechanizmu opisanego w tej części. Najczęściej kwota nagrody jest ustalana w oparciu o sumę, którą udało się odzyskać lub oszczędzić dzięki działaniu sygnalisty. W polskim porządku prawnym należałoby rozważyć możliwość nagradzania sygnalistów, którzy nie są współsprawcami legitymującymi się czynnym żalem w drodze ujawniania informacji o możliwości popełnienia przestępstwa. Wszak takie osoby są nagradzane za swoje zachowanie w drodze złagodzenia odpowiedzialności karnej albo nawet jej wyłączenia. Jednak takie przepisy wymagałyby odpowiednich sankcji karnych za ujawnianie fałszywych informacji czy legitymowanie się złą wiarą, złymi intencjami czy działanie w sposób sprzeczny z zasadami współżycia społecznego.

Odpowiedzialność prawna sygnalistów za przekazywanie fałszywych informacji powinna mieć dwojaki charakter. Z jednej strony tacy pracownicy mogą ponieść odpowiedzialność cywilnoprawną za szkodę spowodowaną swojemu pracodawcy poprzez koszty zbędnego postępowania nadzorczego czy straty wizerunkowe. Wydaje się jednak, że świadome przekazywanie fałszywych informacji powinno być odpowiednio sankcjonowane karnie.

Kompleksowa procedura sygnalizowania nieprawidłowości stanowi element struktury nadzoru wewnętrznego instytucji finansowych. Wiąże się z jego specjalistycznym segmentem, który dla swojej efektywności powinien być odrębną komórką systemu ds. zgodności (Compliance Services)[69]. Oddolna inicjatywa nadzorcza w połączeniu ze spójną siatką zorganizowanego nadzoru zdaje się najskuteczniejszym instrumentem kontroli operacji pracowników instytucji finansowych i przeciwdziałania potencjalnej przestępczości.

---

[68] Więcej: J.V. Butler, D. Serra, G. Spagnolo, *Motivating Whistleblowers*, Departmental Working Papers (2017) 1701, Southern Methodist University, Department of Economics.

[69] Komórki *compliance* zostały związane przez polskiego ustawodawcę w ramach sektora finansowego modelem zgłaszania nieprawidłowości przez sygnalistów.

2.4. Program sygnalistów na przykładzie rozwiązań prawa amerykańskiego w perspektywie prawa polskiego

Istnienie wewnętrznych i zewnętrznych procedur zgłaszania naruszeń przez pracowników podmiotów działających na rynku finansowym pozwala zarówno samym podmiotom, jak i państwowym organom na skuteczne zapobieganie popełnianiu przestępstw. W celu znalezienia optymalnego sposobu regulacji takich procedur zawsze warte wzięcia pod uwagę są doświadczenia innych porządków prawnych[70]. W przypadku przestępczości w instytucjach finansowych staje się to tym bardziej zasadne z uwagi na międzynarodowy charakter rynku finansowego oraz wzajemne zależności i powiązania głównych podmiotów, które na nim działają.

Z tego względu warto, aby polski prawodawca został zapoznany z rozwiązaniami prawa amerykańskiego. Może ono stanowić punkt odniesienia dla regulacji sygnalistów oraz samego mechanizmu informowania czy to danego podmiotu zbiorowego, czy to instytucji publicznych o popełnianych przestępstwach na rynku finansowym. Regulacja amerykańska stanowi o tyle dobry kontekst porównawczy, że wprowadza kontrowersyjne w doktrynie rozwiązanie w postaci nagradzania przez instytucje publiczne osób, które zgłaszają popełnienie przestępstwa finansowego przez dany podmiot zbiorowy. Tego typu polityka prawna jest stosowana już w innych państwach, np. w Kanadzie, lecz co do zasady budzi wątpliwości i przez niektóre państwa jest wprost odrzucana, jak np. przez Wielką Brytanię[71], która jednak stosuje podobne rozwiązanie w przypadku regulacji antykartelowych[72]. Co więcej, coraz częściej dyskutuje się nad zwiększeniem ochrony sygnalistów i poprawieniem ich

[70] J. Polański, *Programy nagradzania informatorów w prawie państw europejskich*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, t. 3, nr 9, s. 9–32; M.C. Vinciguerra, *Whistleblower Protection Legislation and Corruption. European Research Centre for Anti-Corruption and State-Building, Hertie School of Governance, Working Paper No. 52*, Berlin 2018; M. Waszak, *Jak wprowadzenie prawnej ochrony sygnalistów może przyczynić się do rozwoju etyki biznesu w Polsce?*, [w:] *Etyka biznesu – wokół kluczowych zagadnień*, red. R. Sroka, Warszawa 2018, s. 41–48; K. Loyens, W. Vandekerckhove, *Whistleblowing from an International Perspective. A Comparative Analysis of Institutional Arrangements*, „Administrative Sciences" 2018, vol. 8, issue 30, s. 1–16.

[71] M. Iwasaki, *Effects of External Whistleblower Rewards on Internal Reporting*, „Harvard John M. Olin Fellow's Discussion Paper Series" 2018, no. 76, s. 7–8.

[72] J. Polański, *Programy nagradzania…*, s. 17–18.

sytuacji, a przyznawanie im pieniężnych nagród może być jednym z narzędzi, które temu służą[73]. Analiza prawnoporównawcza w tym zakresie bierze pod uwagę także ocenę skuteczności regulacji amerykańskiej na podstawie corocznych raportów oraz dyskusji doktrynalnej, która nabrała większej intensywności w ciągu ostatniej dekady[74]. Wnioski z przedstawionych badań mogłyby zostać wzięte pod uwagę przy ocenie efektywności wprowadzanych obecnie w Polsce regulacji chroniących sygnalistów, którzy informują o przestępstwach popełnianych w ramach działalności podmiotów zbiorowych[75].

W istocie propozycje polskiego prawodawcy, zarówno we wspomnianych regulacjach prawa bankowego, jak i w nowej ustawie o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu ogniskują się wokół tworzenia wewnętrznych programów ochrony sygnalistów, tj. nakładają obowiązek na pracodawców, aby chronili zgłaszających pracowników przed środkami odwetowymi. Z tego powodu tak duży nacisk kładzie się na zapewnienie anonimowości oraz powstrzymanie się przed dyskryminacją ze strony samego pracodawcy. Temu celowi służą także „Standardy" przyjęte przez Giełdę Papierów Wartościowych w Warszawie, które wskazują, jakie warunki ochrony sygnalistów powinny być spełniane przez spółki notowane na tej giełdzie[76]. Pierwszym krokiem w kierunku regulacji zewnętrznego programu sygnalistów, a zatem wprowadzenia możliwości zgłaszania informacji o przestępstwie jako sygnalista do podmiotu zewnętrznego względem instytucji, w której dochodzi do naruszeń, jest projekt ustawy o jawności życia publicznego. Sam projekt

---

[73] S. Wolfe, M. Worth, S. Dreyfus, *Protecting Whistleblowers in the UK. A New Blueprint*, London 2016, s. 22.

[74] M.H. Baer, *Reconceptualizing the Whistleblower's Dilemma*, „UC Davis Law Review" 2017, no. 50, s. 2215–2280; J.P. Near, M.P. Niceli, *After the Wrongdoing. What Managers Should Know About Whistleblowing*, „Business Horizons" 2016, no. 59, s. 105–114; *Why Whistleblowers Wait. Recommendations to Improve the Dodd-Frank Law's SEC Whistleblower Awards Program*, Washington 2018; J.R. O'Sullivan, *„Private Justice" and FCPA Enforcement. Should the SEC Whistleblower Program Include a Qui Tam Provision?*, „American Criminal Law Review" 2016, no. 53, s. 67–115; E.J. Ballan, *Protecting Whistleblowing (and Not Just Whistleblowers)*, „Michigan Law Review" 2017, no. 116, issue 3, s. 475–500.

[75] http://orka.sejm.gov.pl/Druki8ka.nsf/Projekty/8-020-1211-2019/$file/8-020-1211--2019.pdf [dostęp: 9.05.2019].

[76] *Standardy rekomendowane dla systemu zarządzania zgodnością w zakresie przeciwdziałania korupcji oraz systemu ochrony sygnalistów w spółkach notowanych na rynkach organizowanych przez Giełdę Papierów Wartościowych w Warszawie S.A.*, Warszawa 2018, Szerzej na ten temat: https://www.gpw.pl/pub/GPW/files/PDF/Standardy.pdf [dostęp: 1.04.2019].

nadal pozostaje w sferze dyskusji, a przewidziana w nim ochrona sygnalistów ulegała zmianie w ramach procesu konsultacji i uzgadniania. Autorzy wzięli pod uwagę w sposób szczególny obiekcje sformułowane przez Radę Legislacyjną i doprecyzowali, które przepisy karne miałyby zastosowanie analogiczne w przypadku sygnalistów, a ponadto wprowadzili procedurę odwołania od postanowienia prokuratora o odmowie przyznania lub o przyznaniu statusu sygnalisty. Przewidziany w art. 61–66 ustawy model zakłada, że pracownik lub zatrudniony na innych zasadach będzie mógł zgłosić możliwość popełnienia przestępstwa organom wymiaru sprawiedliwości, a następnie o objęciu go programem sygnalisty będzie decydował prokurator jako podmiot chroniący sygnalistę i współpracujący z nim. Przykładowo zwolnienie lub zastosowanie środków odwetowych bez zgody prokuratora narazi pracodawcę na zwiększoną odpowiedzialność odszkodowawczą względem sygnalisty. Pewną wadą tej propozycji jest jednak przerzucenie kwestii ochrony sygnalistów na prokuratorów oraz upodobnienie procedury informowania o możliwych naruszeniach do znanego w prawie zgłoszenia popełnienia przestępstwa. Dużo wreszcie zależy od przyznania sygnaliście ochrony przez prokuratora, a o tym powinno decydować się w oparciu o specjalistyczną wiedzę, która pozwoli albo docenić przedstawione informacje, albo rozpoznać w nich nieuzasadnioną próbę szykanowania pracodawcy.

Dotychczas w praktyce polskiej można wskazać co najmniej dwa przykłady programów informowania zewnętrznego. Pierwszy to zdawkowy program UOKiKu, wykorzystywany do zbierania informacji o działaniach kartelowych, który zostanie oceniony w szerszym kontekście, lecz już należy zaznaczyć, że nie wiąże się z żadną ochroną sygnalisty, poza zapewnieniem pewnej dozy anonimowości. Drugi to nowszy program wprowadzony przez Ministerstwo Inwestycji i Rozwoju w ramach Programu Operacyjnego Infrastruktura i Środowisko na lata 2014–2020. Pozwala on zgłaszać nadużycia w korzystaniu ze środków unijnych bezpośrednio do POIŚ lub na adres e-mail: naduzycia.POIS@miir.gov.pl albo przez specjalny formularz. Co ciekawe, obowiązek informowania o takiej możliwości wpisany jest do umów zawieranych z beneficjentami programu. Zobowiązują się oni do ochrony sygnalistów, a także niestosowania wobec nich środków odwetowych. Punkt ciężkości w przypadku programu POIŚ dalej umiejscowiony jest na ochronie anonimowości, jednakże ewentualna odpowiedzialność umowna beneficjentów stanowi już

pewne narzędzie prawne, które może wpłynąć wymiernie na zachowanie pracodawców. Z punktu widzenia unijnego coraz istotniejsza jest właśnie ochrona sygnalisty. Od pewnego czasu trwają prace na uchwaleniem dyrektywy wprowadzającej obowiązek pewnego minimalnego standardu ochrony sygnalistów w całej Unii Europejskiej. Przedstawiona propozycja dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii z 23.04.2018 r. w istocie przyjmuje wzór ochrony sygnalistów oparty na modelu brytyjskim[77]. Jest on trzystopniowy. W pierwszej kolejności prawodawcy krajowi powinni wprowadzić regulacje, które nakazują tworzenie programów ochronnych dla sygnalistów wewnątrz pracy. W drugiej kolejności sygnaliści powinni mieć możliwość zgłoszenia naruszenia do organów państwowych, jeśli procedury wewnętrzne są nieefektywne bądź ich nie ma. Wreszcie, gdy organy publiczne nie podejmą działań w sprawie zgłoszonych informacji, sygnalista powinien mieć prawo w określonych okolicznościach na powiadomienie mediów i opinii publicznej[78]. Bardzo często, także w USA, najsłynniejsze postaci sygnalistów to właśnie „superbohaterowie", którzy choć piastowali wysokie stanowiska w firmach, postanowili chronić społeczeństwo przed niebezpieczeństwem, ujawniając nieprawidłowości za pośrednictwem mediów[79]. W związku z tym warto, aby polski prawodawca zapoznał się z rozwiązaniami dotyczącymi zewnętrznych programów ochrony sygnalistów, które działają już od dłuższego czasu. Dzięki temu możliwe stanie się wyciągnięcie wniosków z dobrych i nieudanych pomysłów na ukształtowanie pozycji sygnalisty, tak aby nie był w oczach społeczeństwa donosicielem, a sam nie wykorzystywał ochrony w celu nieuczciwej walki z byłym pracodawcą. Co więcej, warto też wziąć pod uwagę rozwiązania, które nie są wprost przewidziane nawet w proponowanych regulacjach unijnych. Wszak obok środków chroniących przed odwetem, na czym wydają skupiać się aktualne europejskie rozwiązania, należy zapytać

[77] Wniosek *Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii z 23.04.2018 r. COM(2018) 218 final 2018/0106(COD)*, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018PC0218 [dostęp: 1.04.2019].

[78] Art. 4 i nn.; art. 6 i nn.; art. 13 Dyrektywy.

[79] A. Epstein, *The NCAA and Whistleblowers. 30–40 Years of Wrongdoing and College Sport and Possible Solutions*, „Southern Law Journal" 2018, no. 28, s. 67.

o zachętę do wzięcia udziału w programie sygnalisty, a zatem należy zastanowić się nad kwestią nagradzania tych, którzy czują się w obowiązku zapobiec przestępnym działaniom i narazić na wszelką formę dyskryminacji.

Zagadnienie ochrony sygnalistów jest analizowane szeroko w doktrynie amerykańskiej już od 30 lat, jednakże tematyka stała się niezwykle nośna po uchwaleniu w 2010 r. ustawy *Dodd-Frank Wall Street Reform and Customer Protection Act*. Jej celem było wprowadzenie nowych środków ochrony rynku finansowego, aby zapobiec kryzysom podobnym do tego, który miał miejsce w 2008 r. Jednym z wielu rozwiązań było ustanowienie programu nagród (*bounty program*) dla sygnalistów informujących o naruszeniach w organizacjach finansowych[80]. Podmiotem odpowiedzialnym za ten program są agencje rządowe – Komisja Papierów Wartościowych i Giełd (SEC) oraz Komisja Rynku Towarów Giełdowych i Kontraktów Futures (CTFC). Rewolucją stała się możliwość udzielania nagród sygnalistom, dzięki pomocy których udało się nałożyć kary na podmioty łamiące w tym zakresie prawo. Program ten skupił uwagę mediów dzięki corocznym raportom, w których szczególnie agencja SEC informuje Kongres o osiągniętych sukcesach. W ostatnim raporcie z roku 2018 Komisja podała, że od początku istnienia Programu (czyli od sierpnia 2011 r.), otrzymała ponad 28 000 zgłoszeń od sygnalistów, a w roku 2018 było ich 5 200. Od początku istnienia Programu Komisja wypłaciła tytułem nagród ponad $326 000 000 dla 59 sygnalistów. W marcu 2018 r. Komisja wypłaciła $50 000 000 wspólnej nagrody dla dwóch osób, co stanowi największą wypłaconą nagrodę; a także $33 000 000 dla innej osoby. Natomiast, we wrześniu 2018 r. Komisja przyznała nagrody w wysokości: $39 000 000 dla jednego sygnalisty i $15 000 000 dla drugiego sygnalisty[81].

Niemniej pomysł na to, aby nagradzać sygnalistów-informatorów nie jest nowy na gruncie amerykańskim. Wcześniej podobny program został ustanowiony w 2006 r. przez Kongres dla urzędu skarbowego i wprowadzony do Kodeksu podatkowego – *Internal Revenue Code § 7623(b)*. Wzorcowe rozwiązanie w kwestii nagród zawiera natomiast najstarszy akt prawny regulujący zagadnienie sygnalistów, tj. *False Claims Act* z 1863 r., nazywany też

[80] M.H. Baer, *op. cit.*, s. 2218.

[81] *2018 Annual Report to Congress. Whistleblower Program*, U.S. Securities and Exchange Commission 2018, s. 9.

„prawem Lincolna" – *Lincoln Law*. W prawie amerykańskim ochrona osób, które informują o naruszeniach dokonywanych wewnątrz organizacji czy to prywatnej, czy to publicznej, regulowana jest na kilka sposobów na poziomie federalnym[82]. Dodatkowo na poziomie stanowym istnieją własne regulacje dotyczące sygnalizowania (*whistleblowing*) i ochrony sygnalistów (*whistleblowers*)[83]. Programy sygnalistów ustanawiane są w ramach wewnętrznych regulacji agencji federalnych odpowiedzialnych za rynek finansowy. Najważniejszy z tych programów realizowany jest przez federalną Komisję Papierów Wartościowych i Giełd Stanów Zjednoczonych – *Program Sygnalistów Komisji Papierów Wartościowych i Giełd Stanów Zjednoczonych*. Ponadto, istnieją programy nagradzające sygnalistów w Urzędzie Skarbowym (*Internal Revenue Service*) oraz w Komisji Rynku Kontraktów Futures. Niezależnie od tego zastosowanie może znaleźć także skarga *qui tam* na podstawie *False Claims Act*, która pozwala osobie prywatnej na wniesienie skargi w imieniu państwa.

Na rynku finansowym znacznie trudniej można korzystać z instrumentu współpracy z organami ścigania, jaki oferuje prawo karne. Zazwyczaj jest ona realna i skuteczna, gdy osobie współpracującej grozi w sposób nieunikniony skazanie za przestępstwo. Wówczas oferta złagodzenia kary albo odstąpienia od jej wymierzenia staje się mocną kartą przetargową i ułatwia pozyskanie cennych informacji o poważnych nadużyciach finansowych danej organizacji. Jednakże uruchomienie procedury współpracy wymaga zebrania uprzednio dowodów, które obciążają potencjalnego współpracującego. W prawie amerykańskim udowodnienie przestępstwa na rynku finansowym jest zaś bardzo trudne, ponieważ wymaga wykazania *mens rea*, a zatem odpowiedniego stanu świadomości sprawcy, co do przestępności popełnianego czynu. Gdy podejrzany zasłania się niepamięcią albo jest przekonany, że podejmował działania biznesowe, bardzo trudno jest odróżnić zachowania przestępne od tych „tylko" ryzykownych, a zatem niemożliwe staje się skazanie, a w konsekwencji atrakcyjna oferta współpracy z organami ścigania – *cooperation agreement*. W wielu przypadkach milczenie jest najczęstszym środkiem

[82] A. Ronickher, *Cybersecurity Whistleblower Protections. An Overview of the Protections and Rewards Available to Cybersecurity Whistleblowers under Federal and State Law*, Washington 2017.

[83] F. Hertel, *Qui Tam For Tax? Lessons from the States*, „Columbia Law Review" 2013, no. 113, s. 1897–1938.

obrony „białych kołnierzyków". Stąd pojawił się pomysł, aby do współpracy zachęcić nagrodami pieniężnymi[84].

Programy nagród dla sygnalistów nie są kluczowym rozwiązaniem, lecz raczej sposobem na domknięcie polityki zapobiegania przestępstwom finansowym. Obok prawa karnego, obok działań operacyjnych, coraz bardziej popularne staje się zachęcanie osób znajdujących się w środku organizacji do dzielenia się informacją bezpośrednio z organami kontrolnymi państwa. Podobne rozwiązania znajdują zastosowanie w przypadku regulacji antymonopolistycznych, a w szczególności służących przeciwdziałaniu kartelom. W tym obszarze program nagród dla sygnalistów jest komplementarnym uzupełnieniem programu *leniency* – łagodzenia kar dla biorących udział w kartelu. W Polsce UOKiK przewiduje w swoim programie, że przedsiębiorca, który uczestniczy w kartelu, jeśli zgłosi zawarcie takiego porozumienia i przedstawi odpowiednie dowody, może ubiegać się o redukcję kar, a nawet całkowite zwolnienie. Analogicznie jak w innych krajach, całkowite zwolnienie dotyczy przedsiębiorcy, który zgłosił się jako pierwszy[85]. Jeśli podobne zgłoszenia zostały dokonane przez kolejnych przedsiębiorców z tego kartelu, przysługują im odpowiednie redukcje kar – zmniejszające się wraz z kolejnością zgłoszeń (najniższa jest obniżka do 20% kary)[86]. Jak wskazuje się w polskiej doktrynie, ewentualny program sygnalistów z opcją nagrody byłby dobrym domknięciem systemu antymonopolowego. Pozwalałby na zachęcanie do ujawniania takich karteli nie tylko przez przedsiębiorców (tylko oni mogą korzystać z *leniency*), lecz także ich pracowników czy byłych pracowników. Nagroda dla osoby fizycznej jest czasami bardziej zachęcająca niż zwolnienie z kary lub jej redukcja dla przedsiębiorcy, jeśli kartel jest trudno wykrywalny i przynosi duże profity. Ponadto, działalność karteli stałaby się bardziej ryzykowna, gdyż wymagałaby większych środków ostrożności ze strony przedsiębiorców w stosunku do własnych pracowników[87]. Rozwiązania w postaci nagród dla sygnalistów w przypadku karteli są już stosowane nie tylko w USA, lecz także w Europie: w Wielkiej Brytanii, na Węgrzech i na Słowacji. Szczegółową analizę porównawczą tych regulacji przedstawił

[84] M.H. Baer, *op. cit.*, s. 2246, 2271.
[85] *Ibidem*, s. 2273.
[86] http://konkurencja.uokik.gov.pl/program-lagodzenia-kar/ [dostęp: 9.05.2019].
[87] J. Polański, *Programy nagradzania…*, s. 27–28.

J. Polański[88]. Uznał on możliwość wprowadzenia nagród dla sygnalistów karteli za ciekawe i nowe rozwiązanie na rynku regulacji antymonopolowych. Wszak UOKiK ma program sygnalistów, lecz bez gratyfikacji pieniężnych, i jedynie z ogólnym komunikatem, że podejmie działania mające na celu *ochronę osób działających jako sygnaliści*[89]. Bez wątpienia jednak program nagród dla sygnalistów to tylko jeden z elementów szerszej polityki przeciwdziałania przestępczości. Na przykładzie ochrony konkurencji widać, że może on przyczyniać się do zwiększenia efektywności pozostałych stosowanych już rozwiązań zapobiegających przestępstwom, jak również stworzyć nowe możliwości walki z nadużyciami finansowymi. Ostrze tego typu programów skierowane jest na uzyskanie wysokiej jakości dowodów na temat przestępstw na dużą skalę. Zrozumiałe jest, że najczęściej adresatem takiej oferty są pracownicy albo byli pracownicy organizacji, które dopuszczają się naruszeń[90]. Stąd zrozumiała jest potrzeba ochrony sygnalistów przed działaniami odwetowymi oraz forma gratyfikacji, która często ma pokryć szkody wynikające z dyskryminacji, której nie da się łatwo udowodnić przed sądem, tj. tej na poziomie społecznym, psychicznym czy rodzinnym[91]. Polski prawodawca zarówno w projekcie ustawy o odpowiedzialności podmiotów zbiorowych, jak i w projekcie ustawy o jawności życia publicznego nie zdecydował się na wprowadzenie programu nagród dla sygnalistów, ograniczając się do zapewnienia różnych narzędzi ochrony przed działaniami odwetowymi[92]. Doświadczenie amerykańskie oraz innych porządków prawnych może zostać zatem wykorzystane w celu przedstawienia modeli stosowanych programów, a także w celu rozeznania zalet i wad oraz szans i ograniczeń tego rozwiązania. Może być to dobry punkt wyjścia lub odniesienia dla ewentualnych projektów mających na celu wprowadzenie podobnych programów w Polsce.

W pierwszej kolejności przedstawione zostaną sposoby ukształtowania programu nagród dla sygnalistów, które stosowane są w prawie

---

[88] *Ibidem*, s. 17–23.

[89] http://konkurencja.uokik.gov.pl/ochrona-sygnalistow/ [dostęp: 9.05.2019].

[90] M.H. Baer, *op. cit.*, s. 2227, 2280.

[91] *Ibidem*, s. 2226.

[92] https://legislacja.rcl.gov.pl/docs//2/12304351/12465401/12465402/dokument313363.pdf [dostęp: 9.05.2019].

amerykańskim. W tym celu zostaną przeanalizowane czynniki, od których zależy forma programu, tj.

1) przedmiot zgłoszenia,
2) wysokość nagrody,
3) podmiot zgłaszający,
4) sposób współpracy z sygnalistą[93].

W drugiej kolejności wskazane zostaną zalety i wady stosowanych rozwiązań na gruncie prawa amerykańskiego, a także szanse i ograniczenia, jakie pojawiają się wraz ze stosowaniem programów nagradzania sygnalistów.

2.5. Struktura programu nagród dla sygnalistów

ad 1) Przedmiot zgłoszenia

False Claims Act – skarga *qui tam*

Najstarszy, a tym samym najbardziej tradycyjny środek prawny, to możliwość wniesienia skargi *qui tam* przez osobę prywatną za działanie na szkodę rządu. Została ona wprowadzona przez prawodawcę na mocy *False Claims Act* jeszcze w 1863 r., aby zapobiegać oszustwom przy dostawach dla rządu amerykańskiego w czasie wojny domowej[94]. Osoba prywatna wnosi skargę w imieniu rządu federalnego, ale dopiero z czasem okaże się, czy rząd podejmie ją i stanie się głównym powodem w sprawie. Nawet jeśli tego nie zrobi, to osoba prywatna może kontynuować proces samodzielnie. Zgodnie z aktualnym brzemieniem FCA skarga musi dotyczyć oszukiwania państwa w celu uzyskania nienależnej zapłaty czy decyzji, przedstawiania fałszywych dokumentów, co powoduje szkodę państwa, niewłaściwego strzeżenia, dostarczania lub certyfikowania odbioru rządowych pieniędzy lub własności; obracania własnością publiczną z nieuprawnionymi urzędnikami czy pomniejszania lub zwalniania ze zobowiązań na rzecz rządu, a także konspirowania w celu popełnienia wszystkich tych aktów[95]. Zatem akt ten chroni przed defraudacją rządowych programów. Przedmiot jest zatem dość szeroki, ale nie

[93] Por. J. Polański, *Programy nagradzania…*, s. 25–30.
[94] A. Epstein, *The NCAA and Whistleblowers…*, s. 65.
[95] FCA § 3729 (a)(1).

jest sprofilowany bezpośrednio na działalność instytucji finansowych, choć dotyczy ich w zakresie, w jakim chodzi o korzystanie ze środków rządowych. Proces toczony jest przed sądem cywilnym, a zatem kończy się zasądzeniem odszkodowania.

Internal Revenue Code § 7623

Wprowadzony w 2006 r. program dotyczy możliwości wypłacenia nagród dla sygnalistów, jeśli pomogli oni w wykryciu zaległości podatkowych lub wykryciu i doprowadzaniu do osądzenia i ukarania osób winnych łamania przepisów podatkowych lub z nimi współdziałających[96]. Przedmiot tego programu ograniczony jest zatem do kwestii wywiązywania się z obowiązków podatkowych, co dla instytucji finansowych, a także dla przestępstw finansowych popełnianych przez przedsiębiorstwa ma duże znaczenie. Ponadto, możliwość skorzystania z pomocy sygnalisty ograniczona jest do spraw, których wartość przekracza $2 000 000[97]. Natomiast w przypadku sprawy przeciwko osobie fizycznej można korzystać z tego programu, jeśli jej całkowity dochód przekracza $200 000 w jakimkolwiek roku podatkowym, którego dotyczy oskarżenie[98]. Zatem już na przykładzie tego programu jasne jest, że IRS interesuje się współpracą z sygnalistami w sprawach poważnych naruszeń podatkowych, z których wpływy do budżetu będą wysokie, a tym samym i nagroda dla sygnalisty większa. Próba zmniejszenia wartości spraw do $20 000 nie zyskała poparcia w Kongresie. Limit dochodu osób fizycznych jest mniej zrozumiały, gdyż przy zaległościach powyżej $2 000 000 dochód roczny zazwyczaj jest raczej wyższy niż $200 000. Niemniej, suma ta wskazuje, że chodzi o ograniczenie zgłoszeń do osób lepiej zarabiających. Co warte podkreślenia, w ramach programu mogłyby nie zostać zaliczone np. sprawy dotyczące podatku spadkowego, gdy wartość otrzymanego przysporzenia przekracza limit ustawowy, a dochody roczne beneficjenta są mniejsze od wymaganych ustawą[99].

---

[96] IRC § 7623 (a)(1)(2).

[97] IRC § 7623(b)(5)(B).

[98] IRC § 7623(b)(5)(A).

[99] E.A. Morse, *Whistleblowers and Tax Enforcement. Using Inside Information to Close the Tax Gap*, „Akron Tax Journal" 2009, vol. 24, s. 18.

Dodd-Frank Wall Street Reform and Customer Protection Act, sec. 922

Ustawa z 2010 r. wprowadziła dodatkowe środki ochrony sygnalistów informujących o przestępstwach na rynku finansowym, a przede wszystkim ustanowiła program nagród dla sygnalistów w ramach Komisji Papierów Wartościowych i Giełd. Zgodnie z ustawą przedmiotem zgłoszenia mają być naruszenia tej ustawy przekazywane Komisji zgodnie z regułami przez nią ustalonymi. W *Security Exchange Act of 1934 sec. 21F* zostało uregulowane w definicji *whistleblower*, że w kręgu zainteresowań Komisji są możliwe naruszenia federalnego prawa papierów wartościowych. W ostatecznych regułach wydanych przez SEC w *Section 21F of the Securities Exchange Act of 1934* w § 240.21F-2[100] zostało wskazane, że przedmiotem zgłoszenia mogą być już dokonane naruszenia prawa papierów wartościowych (w tym wszelkie zasady i regulacje); naruszenia, które aktualnie są dokonywane; albo naruszenia, które są planowane i mogą nastąpić. Zatem zakres przedmiotowy programu sygnalistów SEC jest bardzo szeroki i obejmuje wszelkie naruszenia federalnego prawa papierów wartościowych – *federal securities laws.* Komisja na swojej stronie internetowej podaje przykładowe naruszenia, które są w kręgu zainteresowania:

- Schemat Ponziego i inne schematy piramid finansowych lub HYIP programy inwestycyjne o wysokiej stopie zwrotu, głównie stosowane w internecie,
- Kradzież lub sprzeniewierzenie funduszy lub papierów wartościowych,
- Manipulacja ceną lub wolumenem papierów wartościowych,
- Wykorzystywanie informacji poufnych,
- Nieuczciwe lub niezarejestrowane oferty papierów wartościowych,
- Fałszywe lub wprowadzające w błąd oświadczenia dotyczące firmy (w tym nieprawdziwe lub wprowadzające Komisję w błąd raporty lub oświadczenia finansowe),
- Nadużywanie krótkiej sprzedaży bez pokrycia,
- Korupcja lub niewłaściwe płatności dla zagranicznych urzędników,
- Nieuczciwe działania związane z transakcjami na papierach wartościowych lub publicznymi planami emerytalnymi,

[100] https://www.sec.gov/about/offices/owb/reg-21f.pdf [dostęp: 9.05.2019].

- Inne oszukańcze działania z udziałem papierów wartościowych[101].

Program SEC jest zatem najbardziej sprofilowany na naruszenia na rynku finansowym. Podobnie jak w przypadku regulacji IRS istnieje także ograniczenie dotyczące wartości sprawy. W przypadku programu SEC wartość kar, które mogą zostać nałożone na naruszającego prawo, musi przekraczać $1 000 000[102]. Prawodawca jest zatem zainteresowany dużymi naruszeniami prawa, które w sposób istotny mogą wpłynąć na stabilność rynku finansowego. W świetle przytoczonych już danych o wysokości wypłacanych nagród, przyjęte przez Komisję sprawy są warte zazwyczaj znacznie więcej niż ustawowy limit, skoro np. zagraniczny sygnalista w ostatnim pozytywnie rozpoznanym wniosku przez SEC uzyskał ok. $ 4 000 000 samej nagrody[103].

Dodd-Frank Wall Street Reform and Customer Protection Act, sec. 748

Ustawa z 2010 r. wprowadziła bliźniaczą regulację dla sygnalistów w przypadku rynku towarów giełdowych – *Commodity Exchange*. Szczegółowa regulacja została zawarta w *Commodity Exchange Act sec. 23*. Zgodnie z regułami programu (§ 165.1) ustalonymi przez agencję federalną – Komisję Rynku Kontraktów Futures i Opcji przedmiotem zgłoszeń są naruszenia ustawy *Commodity Exchange Act*. Podobnie jak w przypadku rynku papierów wartościowych wartość kar, które mogą zostać nałożone na podmiot naruszający, musi przekroczyć $1 000 000[104].

Podsumowując, w prawie amerykańskim stosowane są różne programy sygnalistów, które dotyczą odmiennych przedmiotowo spraw. Zdecydowanie najogólniejszy przedmiot ma skarga *qui tam*, która dotyczy sprzeniewierzenia funduszy rządowych. Charakterystyczna rola została przypisana sygnalistom w ramach prawa podatkowego, gdzie celem programu jest pozyskiwanie informacji o naruszeniu obowiązków podatkowych. Wreszcie regulacje najbardziej związane z rynkiem finansowym za swój główny przedmiot wzięły przestępstwa dotyczące rynku papierów wartościowych oraz rynku towarów

[101] https://www.sec.gov/whistleblower/frequently-asked-questions#faq-1 [dostęp: 9.05.2019]; 2018 *Annual Report*..., s. 17, https://www.sec.gov/files/sec-2018-annual-report-whistleblower-program.pdf [dostęp: 9.05.2019].

[102] Sec. 21F(a)(1).

[103] https://www.sec.gov/news/press-release/2018-209 [dostęp: 9.05.2019].

[104] Section 23 of the Commodity Exchange Act (7 U.S.C. § 26)(a)(1).

giełdowych, szczególnie kontraktów futures i opcji. Warte zaznaczenia, że najnowsze programy wprowadzają określoną minimalną wartość sprawy, w której program sygnalistów może zostać wykorzystany i zazwyczaj jest ona duża, tj. od min. $1 000 000 lub od min. $2 000 000. Z jednej strony, jest to podyktowane efektywnością programów, aby liczba rozpatrywanych spraw nie przekroczyła możliwości skutecznego działania odpowiedzialnych organów. Z drugiej strony, wprowadzenie takiego wymogu w znaczący sposób wpływa na wysokość uzyskiwanych przez sygnalistów nagród.

ad 2) Wysokość nagrody

False Claims Act – skarga *qui tam*

W pierwszej wersji ustawy z 1863 r. (FCA § 3729 sec. 6) sygnalista uprawniony był do 50% sumy, którą rządowi udało się odzyskać (*forfeitures*) w wyniku rozpoczętego przez sygnalistę procesu, oraz do 50% sumy odszkodowania (*damages*), która została zasądzona. W 1986 r. wprowadzony został nowy model ustalania wysokości nagrody, który wpłynął następnie na kształt regulacji Kodeksu podatkowego IRC oraz programów nagród wprowadzonych przez *Dodd Frank Act*. Od 1986 r. wysokość nagrody zależy w pierwszej kolejności od tego, czy rząd podjął sprawę rozpoczętą przez sygnalistę, czy też nie zdecydował się na dołączenie do niej, pozostawiając jej losy w rękach osoby fizycznej. Jeśli rząd przejął sprawę, to sygnalista dostaje od 15% do 25% wysokości zasądzonego i wyegzekwowanego wyroku lub wysokości zawartej ugody. Sąd wskazuje odpowiedni udział sygnalisty w zależności od tego, jak bardzo skarżący przyczynił się do sukcesu wyroku – FCA § 3729 (d)(1). Jednakże, jeśli informacje wskazane jako podstawa skargi były znane sygnaliście z innych źródeł: procesów, akt procesowych, raportów, etc., a nie dostarczył on oryginalnie własnej informacji, wówczas sąd ustala właściwą kwotę nagrody, ale nie więcej niż 10% wysokości wyroku. W tym przypadku zatem o stopniu przyczynienia się do sukcesu może decydować również stopień oryginalności materiałów dowodowych dostarczonych przez sygnalistę.

Natomiast, jeśli rząd nie podjął sprawy, to skarżący może liczyć na większą nagrodę, tj. od 25% do 30% wysokości wyroku lub ugody – FCA § 3729(d)(2). W każdym przypadku koszty procesowe i reprezentacji prawnej zwraca pozwany, a państwo nie jest w żaden sposób zobowiązane wobec sygnalisty.

Internal Revenue Code § 7623

Osoba, która powiadomiła o nadużyciach podatkowych, może uzyskać nagrodę wynoszącą od 15% do 30% wpływów, jakie z tego postępowania uzyskał IRS[105]. Wielkość udziału zależy od stopnia rzeczywistego przyczynienia się do sukcesu podjętego w związku z informacją postępowania oraz skuteczności egzekucji nałożonych kar. Wysokość nagrody zmniejsza się, gdy sygnalista opierał się na informacjach dostępnych publicznie albo sam zaplanował lub zainicjował działania, które doprowadziły do naruszenia prawa podatkowego. Zatem nagroda w istocie nie jest wypłacana z budżetu IRS, tylko pokrywana jest z egzekwowanych kar nałożonych na oskarżonego. Wypłata następuje po zakończeniu całego postępowania, po uprzednim przedstawieniu ustalenia przez IRS wysokości nagrody. Sygnaliście przysługuje w tym zakresie odwołanie do sądu podatkowego (*US Tax Court*).

Dodd-Frank Wall Street Reform and Customer Protection Act, sec. 922, sec. 748

Wysokość nagrody regulowana jest przez § 240.21F-5. Co do zasady wysokość jest ustalana swobodnie przez Komisję. Decyduje ona każdorazowo o tym, jaki procent kary będzie wyznaczał wysokość nagrody. Nie może być ona jednak niższa niż 10% i wyższa niż 30% kary, którą Komisja lub inne podmioty mogą wyegzekwować od podmiotu naruszającego prawo. W przypadku, gdy więcej niż jeden sygnalista jest uprawniony do nagrody, Komisja wyznaczy indywidualnie każdemu wysokość nagrody. Niemniej, łączna wysokość wypłaconych nagród wszystkim sygnalistym też nie może wykraczać poza wskazany zakres (10–30%).

W § 240.21F-6 wskazane są kryteria, które mogą wpływać na ustalaną wysokość nagrody. Wysokość nagrody może zwiększać znaczenie przekazanej informacji:

- stopień wiarygodności, kompletności i wpływ na egzekucję kary i wysokość środków, które udało się Komisji zabezpieczyć;
- stopień, w jakim informacja przyczyniła się do pozytywnego rozpatrzenia roszczeń wniesionych do Komisji.

Ponadto, istotna jest pomoc ze strony sygnalisty: w jakim stopniu współpracował z Komisją, czy był gotowy do przedstawiania wyjaśnień,

[105] IRC § 7623(b)(1).

do odzyskiwania środków finansowych, które jeszcze nie zostały stracone w wyniku przestępnych działań, a także bierze się pod uwagę wszystkie wyjątkowe niedogodności, które spotkały sygnalistę w wyniku pomagania Komisji w likwidacji naruszenia prawa.

Wreszcie, liczy się interes organów ścigania, tj. w jakim stopniu przyznana nagroda może przyczynić się do lepszego wykrywania przestępstw, do egzekwowania prawa, do pozyskiwania wysokiej jakości informacji, a tym samym może pomóc w realizowaniu priorytetów Komisji, a także w jakim stopniu wykryte naruszenie zagrażało inwestorom.

Prawodawca podkreśla, że wysokość nagrody jest większa, jeśli sygnalista korzystał z wewnętrznego programu *compliance* podmiotu oskarżonego. Zatem Komisja bada, czy sygnalista zgłosił naruszenie do właściwej wewnętrznej komórki podmiotu wcześniej lub w tym samym czasie, co Komisji; czy pomagał i współpracował w wewnętrznych procedurach lub dochodzeniach, które dotyczyły zgłaszanych naruszeń.

Regulacja SEC wskazuje także czynniki, które mogą spowodować zmniejszenie wysokości nagrody. Wśród nich jest stopień zawinienia sygnalisty: jego rola w zgłoszonych naruszeniach. Bierze się pod uwagę wiedzę, doświadczenie, stan przeszkolenia i stanowisko sygnalisty w czasie występowania naruszeń prawa. Istotne jest, czy działał ze świadomością popełniania naruszenia, czy zgadzał się na te naruszenia, zarówno ogólnie, jak i w przypadku konkretnych osób. Ponadto, Komisja ustala, czy zyskał finansowo na dokonanych naruszeniach; czy jest recydywistą; a także, jaki jest stopień społecznej szkodliwości popełnionego przez sygnalistę przestępstwa.

Kolejny czynnik, który może wpłynąć na zmniejszenie wysokości nagrody, to nieuzasadnione opóźnienie w zgłoszeniu informacji. Wreszcie w programie SEC dba się o to, aby program federalny nie wpłynął negatywnie na przestrzeganie wewnętrznych procedur stosowanych w przedsiębiorstwach, które mają służyć przeciwdziałaniu przestępczości[106]. Stąd negatywnie na wysokość nagrody może wpłynąć jakakolwiek ingerencja sygnalisty w wewnętrzny program *compliance* lub system kontroli wewnętrznej: czy ingerował w wewnętrzne procedury, aby opóźnić lub uniemożliwić wykrycie naruszeń; czy fałszował, kłamał lub tuszował informacje, dostarczał fałszywe

[106] M.H. Baer, *Reconceptualizing…*, s. 2232.

pisemne oświadczenia, dokumenty, co nie pozwalało na wykrycie i usunięcie naruszeń przez wewnętrzne organy podmiotu.

W programach sygnalistów SEC i CFTC wskazane zostały szczegółowo przesłanki, jakie muszą spełnić dostarczone informacje, aby uzyskanie nagrody stało się bardziej prawdopodobne. Przede wszystkim Komisja uznaje, że sygnalista „dobrowolnie" przekazał informację, jeśli stało się to, zanim skierowano do tej osoby albo do jej pełnomocnika żądanie, pytanie czy prośbę o informację związaną z przedmiotem zgłoszenia. Ponadto, zgłoszenie takiej informacji nie może wynikać z uprzednio istniejącego prawnego obowiązku zgłoszenia (np. w ramach audytu czy zespołu ds. *compliance*) albo innego obowiązku umownego, np. w stosunku do komisji SEC czy CFTC.

Za „oryginalną" uznaje się informację, która wynika z własnej, niezależnej wiedzy lub jest wynikiem własnej analizy. Nie powinna być oparta tylko na powszechnie dostępnej wiedzy, lecz na własnych doświadczeniach, wiadomościach, obserwacjach. Prawodawca wyłączył z tego zakresu informacje, które są objęte tajemnicą adwokacką lub jeśli osoba pozyskała je za pomocą środków lub w sposób, który jest sprzeczny z regułami właściwego federalnego lub stanowego prawa karnego. Wreszcie istotny jest tu czynnik pierwszeństwa, tj. że informacja nie była uprzednio zgłoszona Komisji przez inne osoby, chyba że później zgłaszający jest źródłem informacji uprzednio zgłoszonych już do Komisji przez inne osoby. Podobnie jak w przypadku regulacji *False Claims Act* istotne znaczenie ma to, żeby informacja nie była oparta wyłącznie na zarzutach formułowanych w postępowaniach sądowych, administracyjnych, raportach rządowych, przesłuchaniach, kontrolach, dochodzeniach albo w doniesieniach prasowych, chyba że zgłaszający jest pierwszym źródłem takich informacji.

Najistotniejsze z punktu widzenia otrzymania nagrody jest to, aby przekazane informacje doprowadziły do skutecznego działania Komisji, czy to przed sądem federalnym, czy administracyjnym, w którego rezultacie zostanie nałożona kara finansowa w wysokości ponad $1 000 000. Stanie się tak z pewnością, gdy przekazana informacja była wystarczająco szczegółowa, wiarygodna i dostarczona na czas, aby możliwe było rozpoczęcie lub wznowienie procedury nałożenia kary. Komisja będzie oceniała, czy informacja dostarczona przez sygnalistę znacząco przyczyniła się do sukcesu już prowadzonego postępowania. Ponadto, informacja powinna zostać przekazana

w pierwszej kolejności albo w tym samym czasie w ramach wewnętrznego programu sygnalistów w miejscu pracy, albo do wewnętrznej komórki ds. *compliance*. Jeśli w wyniku tego zgłoszenia podmiot sam zgłosił informację do Komisji; albo gdy wewnętrzna komórka ds. *compliance* przekazała Komisji wyniki kontroli rozpoczętej na podstawie zgłoszenia sygnalisty, a ten dostarczył taką samą informację Komisji w ciągu 120 dni od zgłoszenia jej w miejscu pracy, to nadal przysługuje mu prawo do nagrody.

ad 3) Podmiot zgłaszający

Jeśli chodzi o zakres podmiotów, które mogą być chronione jako sygnaliści, istnieje duża rozbieżność między czterema analizowanymi regulacjami. W przypadku *False Claims Act* skargę cywilną może wnieść osoba fizyczna – FCA § 3729 (b)(1), bez jakichkolwiek dodatkowych ograniczeń. Naturalnie nie każdy, kto wystąpi z taką skargą, będzie automatycznie uznany za osobę uprawnioną do uzyskania nagrody. Jeśli zgłaszający został skazany za naruszenia, które były przedmiotem wniesionej przez niego skargi *qui tam*, jest odsuwany od sprawy i nie otrzyma żadnych nagród, ale postępowanie cywilne może kontynuować rząd. W przypadku, gdy skarżący sam kontynuował proces i przegrał, to sam pokrywa zasądzone koszty, a także wypłaca ewentualne odszkodowanie pozwanemu, jeśli okaże się, że zgłoszona przez niego skarga była frywolna, wyraźnie dokuczliwa; albo wniesiona tylko w celu szykanowania.

Analogicznie zakreślony jest status podmiotowy w regulacji podatkowej IRC. Uprawniona do złożenia informacji o naruszeniach prawa podatkowego jest każda osoba fizyczna. Jednakże w sytuacji, gdyby została skazana w postępowaniu karnym za zaplanowanie lub zainicjowanie działań, które są objęte przedmiotem regulacji: doprowadziły do zaległości podatkowych albo do innych naruszeń prawa podatkowego lub współdziałały w nich, nie przysługuje jej nagroda.

Natomiast w przypadku programu SEC prawodawca zdecydował się na dużo bardziej złożoną regulację podmiotów, które mogą uczestniczyć w programie nagród. Profil sygnalisty został tak ukształtowany, aby nie wpływać negatywnie na inne środki prawne skierowane przeciwko przestępczości finansowej, a być raczej narzędziem komplementarnym wobec nich. Program wyraźnie określa, że *eligible whistleblower* może być osoba, która dobrowolnie

dostarcza oryginalną informację o możliwym naruszeniu federalnego prawa papierów wartościowych. Sygnalistą może być tylko osoba fizyczna, ale informację o naruszeniu może też złożyć kilka osób wspólnie. Takie sytuacje zdarzają się, o czym świadczy raport SEC z 2018 r. Komisja nie wymaga, aby zgłaszający był pracownikiem podmiotu, którego dotyczy zgłoszenie naruszenia prawa, choć najczęściej wśród nagrodzonych sygnalistów są aktualni albo byli pracownicy takich podmiotów. Niemniej, krąg sygnalistów nie jest tak szeroki jak może się wydawać. W regulacji programu wyraźnie wskazano, kto nie może być sygnalistą. Przede wszystkim wyłączone z tego programu są osoby sprawujące funkcje kierownicze, które odpowiadają za działania podmiotu zbiorowego i mają wpływ na ich przebieg, a zatem dotyczy to: dyrektorów, kierowników, członków zarządu, wspólników podmiotu, którym została zgłoszona taka informacja o nieprawidłowościach w podmiocie; albo jeśli pozyskali oni takie informacje w ramach wewnętrznych procedur mających na celu identyfikowanie, zgłoszenie i reakcję na występujące naruszenia prawa. Racjonalne jest, aby mając taką informację, nie uczestniczyli w programie sygnalistów, tylko podjęli działania w zakresie swoich kierowniczych stanowisk. Ten sam argument legł u podstawy wyłączenia z programu sygnalistów pracownika, którego głównym obowiązkiem jest kontrola przestrzegania prawa w firmie (np. członka zespołu ds. *compliance*) albo prowadzenie audytu wewnętrznego, jak również, jeśli zgłaszający nie jest bezpośrednim pracownikiem takiej organizacji, lecz został zatrudniony lub jest w inny sposób powiązany z firmą, której zlecono prowadzenie wewnętrznej kontroli przestrzegania prawa (*compliance*) albo prowadzenie audytu wewnętrznego w tymże podmiocie. Ponownie chodzi tu o wyeliminowanie swoistego konfliktu interesów i promowanie korzystania z dostępnych procedur, zamiast uciekania się do bezpośredniego kontaktu z SEC. Osoby sprawujące takie funkcje mają narzędzia i środki, aby prowadzić skuteczną walką z naruszeniami. Z tych samych powodów informacji o naruszeniach w programie sygnalistów nie może wykorzystywać osoba zatrudniona lub w inny sposób powiązana z firmą, której zlecono dochodzenie w sprawie wykrycia możliwych naruszeń prawa w danym podmiocie. Jak również osoba, która została zatrudniona lub jest w inny sposób powiązana z firmą, zajmującą się publiczną rachunkowością, jeśli pozyskała informacje o naruszeniach prawa przy prowadzeniu kontroli rachunkowości publicznej

w podmiocie (jest czymś innym niż audyt w świetle prawa amerykańskiego). W ten sposób regulacja programu sygnalistów pragnie zapobiec nadużywaniu programu nagród i zaniechaniu prowadzenia innych praktyk promowanych przez prawodawcę, jak tworzenie procedur *compliance*, dokonywanie audytów wewnętrznych czy kontroli rachunkowości publicznej. Z tego powodu również ci, którzy otrzymali informację o naruszeniach od powyższych osób, nie mogą być sygnalistami.

Wyłączenie z programu sygnalistów tych osób nie jest jednak absolutne. Osoby trzecie mogą uczestniczyć w programie sygnalistów, jeśli informacja, którą otrzymali od wyłączonych osób, dotyczy naruszeń, w które powyższe osoby mogą być zamieszane albo dotyczy informacji, które powyższe osoby mogą zgłosić w ramach Programu. Regulacja dopuszcza bowiem przypadki, w których wskazane wcześniej osoby mogą zostać dopuszczone do bycia sygnalistami. Po pierwsze, jest to możliwe, jeśli taka osoba ma uzasadnioną podstawę (*reasonable basis*), aby sądzić, że zgłoszenie informacji do Komisji jest konieczne, aby uniemożliwić działania, które mogą bardzo prawdopodobnie wyrządzić poważną szkodę (*likely to cause substantial injury*) interesowi finansowemu podmiotu lub jego majątkowi lub jego inwestorom. Po drugie, jeśli taka osoba ma uzasadnioną podstawę (*reasonable basis*), aby sądzić, że podmiot podejmuje działania, które doprowadzą do uniemożliwienia wykrycia dokonanego naruszenia w przyszłości. Po trzecie, jeśli minęło co najmniej 120 dni od zgłoszenia przez taką osobę informacji o naruszeniu wewnątrz firmy właściwemu zespołowi, który zajmuje się audytem wewnętrznym, dyrektorowi działu prawnego, dyrektorowi komórki ds. *compliance* (lub odpowiednikowi), własnemu przełożonemu. Podobnie dzieje się, jeśli minęło 120 dni od momentu, gdy ta osoba otrzymała informację o naruszeniu, i okoliczności wskazywały, że o tym naruszeniu wiedzą również: zespół, który zajmuje się audytem wewnętrznym, dyrektor działu prawnego, dyrektor komórki ds. *compliance* (lub odpowiednik) lub jej własny przełożony.

ad 4) Sposób współpracy z sygnalistą i jego ochrony

Procedura przewidziana w *False Claims Act* zakłada całkowitą jawność osoby sygnalisty. Wszak to on sam wytacza powództwo przeciwko konkretnej organizacji lub osobie. Ponadto, jest to postępowanie cywilne, zatem niesie znacznie mniej dotkliwe skutki niż postępowanie karne, tj. ogranicza się do

wypłacenia odszkodowania państwu oraz ewentualnie samemu sygnaliście, jeśli on również poniósł straty. Państwo nie pokrywa kosztów poniesionych przez sygnalistę, a jest odpowiedzialne za wypłacenie nagrody, co do której ma dużą dyskrecjonalność, czy wypłaci i w jakiej wysokości. Ponadto, do państwa należy decyzja, czy wytoczony proces należy kontynuować. Co więcej, nie musi wspierać wytoczonego powództwa. W związku z tym, jak wskazuje się w literaturze, największym zagrożeniem w przypadku skargi *qui tam*, jest to, czy państwo w ogóle zainteresuje się sprawą[107].

Osoba prywatna składając skargę *qui tam*, występuje publicznie w obronie państwa, przez co naraża się na działania odwetowe ze strony powoda lub osób z nim związanych. Z tego względu zrozumiałe jest, że państwo musi podjąć się obrony sygnalisty przed działaniami odwetowymi. *False Claims Act* przewiduje możliwość wniesienia skargi na podstawie tej ustawy do sądu federalnego. Ochronie podlega sygnalista, który jako pracownik, wykonawca, agent lub w jakikolwiek inny sposób zatrudniony u pozwanej osoby lub organizacji, został zwolniony, zdegradowany, zawieszony, zastraszony, nękany lub w jakikolwiek inny sposób dyskryminowany w zakresie warunków zatrudnienia ze względu na wysiłki w celu powstrzymania przestępstw wymienionych w *False Claims Act*. Na podstawie tej ustawy sygnalista może żądać przywrócenia na stanowisko o tej samej randze; podwójnego zaległego wynagrodzenia; odszkodowania za szkody wynikające z dyskryminacji, w tym koszty adwokatów i koszty procesowe. Skarga jest ograniczona czasowo – sygnalista może ją wnieść w ciągu 3 lat od wystąpienia działań odwetowych.

W przypadku regulacji Kodeksu prawa podatkowego IRC sygnaliści nie są w żaden sposób chronieni przed działaniami odwetowymi. Chociaż IRS wskazuje w swoich corocznych raportach, że stara się dbać o utrzymanie w tajemnicy tożsamości oraz samego istnienia sygnalistów, to jednak aktualna regulacja IRC nie daje właściwych narzędzi w tym celu. Stanowi to niewątpliwie dużą bolączkę, która może odstraszać przed korzystaniem z programu sygnalistów tych, którzy są aktualnymi pracownikami w podmiotach, o których przestępnej działalności chcieliby poinformować organy podatkowe.

Zupełnie odmiennie wygląda pod tym względem program sygnalistów SEC i CFTC. Zasady współpracy z sygnalistą są ściśle określone zarówno pod

[107] *Ibidem*, s. 2252.

względem sposobu zgłaszania informacji, jak i ochrony jego tożsamości oraz środków prawnych na wypadek działań odwetowych wobec niego. Zgodnie z §240.21F-9 reguł programu SEC sygnalista ma trzy sposoby na zgłoszenie informacji. Po pierwsze, za pośrednictwem specjalnie przygotowanej strony internetowej, na której wypełnia się stosowny formularz zgłoszenia skargi Form TCR (*Tip*, *Complaint or Referral*). Po drugie, wysyłając wypełniony formularz listownie lub faxem na adres Komisji. Po trzecie, może zachować swoją anonimowość, zgłaszając informację tylko za pośrednictwem prawnego pełnomocnika. Ponadto, Komisja zobowiązuje się, że nie będzie udzielała informacji o sygnaliście, nawet w przypadku żądań w oparciu o prawo do informacji publicznej. Podobnie jak w przypadku zgłoszenia informacji organom podatkowym IRS, wymagane od sygnalisty jest oświadczenie pod groźbą odpowiedzialności karnej, że podana informacja jest prawdziwa i poprawna, przedstawiona zgodnie z najlepszą wiedzą i w najlepszym przekonaniu. Z uwagi na to, że nagroda, podobnie jak w pozostałych dwu procedurach wypłacana jest ze środków wyegzekwowanych od podmiotów, które dopuściły się naruszeń prawa, sygnalista jest zmuszony czekać na wypłatę ewentualnej nagrody aż do zakończenia egzekucji. Gdy ona nastąpi, Komisja informuje o nałożonych karach oraz wzywa publicznie do złożenia wniosków o przyznanie nagrody. Wszyscy, którzy uznają, że może to dotyczyć zgłoszonych przez nich informacji jako sygnalistów, składają odpowiednie wnioski, w których już ujawniają swoją tożsamość. Komisja następnie ocenia złożone wnioski i podejmuje decyzję, komu wypłaci nagrodę oraz w jakiej wysokości. Jeśli wnioskodawcy nie zgadzają z ustaleniem Komisji, czy co do odrzucenia wniosku, czy nieodpowiedniej wysokości nagrody, mogą wnieść odwołanie do właściwego sądu.

W zakresie ochrony sygnalisty przed działaniami odwetowymi regulacja przyznaje dogodniejsze uprawnienia[108]. Przewiduje, że sygnalista może wnieść pozew bezpośrednio do sądu federalnego, a Komisja jest uprawniona do rozpoczęcia procedury egzekucyjnej przeciwko pracodawcy, jeśli ten zwolnił, zawiesił, przeniósł na niższą pozycję, w sposób bezpośredni lub pośredni zastraszał, nękał albo dyskryminował w jakikolwiek inny sposób sygnalistę za dostarczenie informacji w ramach Programu sygnalisty albo za pomaganie

[108] *Ibidem*, s. 2225.

w prowadzonym dochodzeniu albo postępowaniu, które rozpoczęło się na podstawie jego informacji. Sygnalista może żądać przywrócenia na tę samą pozycję w pracy; sumy zaległych pensji, które sygnalista otrzymałby, gdyby nie dyskryminacja, wraz z odsetkami; odszkodowania za jakiekolwiek szkody, które sygnalista poniósł w wyniku zwolnienia i dyskryminacji, wraz z kosztami procesowymi, kosztami opinii biegłych czy racjonalnych kosztów zastępstwa procesowego.

2.6. Zalety i wady programów sygnalistów

W doktrynie amerykańskiej nowe rozwiązanie w postaci federalnego programu sygnalisty przyczyniło się do dyskusji nad relacją między zewnętrznym programem sygnalistów a wewnętrznymi programami sygnalistów, wprowadzanymi przez samych pracodawców[109]. Czy istnienie zewnętrznego programu, który oferuje nagrody za zgłaszanie naruszeń prawa wewnątrz podmiotów, działających na rynku finansowym, nie zniechęci do korzystania z wewnętrznych procedur walki z przestępczością, czy nie sprzeciwi się wprowadzanym wymogom dbania przez samych przedsiębiorców o działania zgodne z prawem i tworzenie wewnętrznych komórek ds. *compliance* czy audytu wewnętrznego? Główna obawa bierze się z nagrody pieniężnej, która ustanowiona została przez amerykańską Komisję (SEC). Wszak w procedurach wewnętrznych raczej nie spotyka się gratyfikacji finansowych za zgłoszenie naruszeń, a sam fakt zgłaszania ma wymiar działania na korzyść firmy, a nie na korzyść osoby zgłaszającej, a zatem nie spotyka się z gratyfikacją niepieniężną.

Za wprowadzaniem nagród pieniężnych w zewnętrznych programach wsparcia sygnalistów przemawiają jednak zarówno argumenty doktryny, jak i dotychczasowe doświadczenia porządku amerykańskiego.

Zgodnie z raportem Komisji (SEC) za rok 2018, aż ok. 83% sygnalistów, którzy otrzymali nagrodę pieniężną za zgłoszenie naruszeń, a byli aktualnymi albo byłymi pracownikami w podmiotach, których dotyczyło zgłoszenie, zgłosiło również informacje o naruszeniach prawa do swoich przełożonych,

[109] M. Iwasaki, *op. cit.*, s. 2–3.

do komórek ds. *compliance* lub za pomocą procedur kontroli wewnętrznej, bądź zrozumieli, że ich przełożeni lub osoby odpowiedzialne mają wiedzę o naruszeniach, zanim zgłosili informację o naruszeniach do Komisji[110]. Co ciekawe, wyniki te zbiegają się z badaniami statystycznymi kilku tysięcy pracowników sektora prywatnego przeprowadzonymi w 2012 r. przez Ethics Resource Center. Zgodnie z uzyskanymi danymi tylko 18% zdecydowało się na skorzystanie z zewnętrznego programu sygnalistów. Natomiast 84% spośród tych, którzy się na to zdecydowali, najpierw zgłosiło naruszenie w wewnętrznej procedurze[111].

W 2018 r. najwięcej zgłoszeń do Komisji SEC dotyczyło: oferowania oszustw finansowych – 20%; przedstawiania Komisji SEC fałszywych informacji lub informacji, które mogą wprowadzać w błąd na temat stanu finansów, rezultatów finansowych, etc. – 19%; manipulacji finansowych – 12%. Warto przypomnieć, że od początku istnienia Programu (czyli od sierpnia 2011 r.), Komisja otrzymała ponad 28 000 zgłoszeń od sygnalistów, a w roku 2018 było ich 5 200. Od początku istnienia Programu Komisja wypłaciła tytułem nagród ponad $326 000 000 dla 59 sygnalistów. W marcu 2018 r. Komisja wypłaciła $50 000 000 wspólnej nagrody dla dwóch osób, co stanowi największą wypłaconą nagrodę; a także $33 000 000 dla innej osoby. Natomiast, we wrześniu 2018 r. Komisja przyznała nagrody w wysokości: $39 000 000 dla jednego sygnalisty i $15 000 000 dla drugiego sygnalisty.

Jednakże, jak słusznie podnosi M.H. Baer, dane te wcale nie napawają optymizmem. Istnieje ogromna dysproporcja między liczbą zgłoszonych naruszeń a liczbą przyznanych nagród – osoby nagrodzone stanowią tylko 0,2%[112]. Wydaje się, że z jednej strony program nie jest interesujący dla grupy docelowej (pracowników z dobrymi dowodami), a z drugiej – rozbudza nadzieje w osobach, które chciałyby zdobyć nagrodę, lecz nie mają wystarczająco dobrego dostępu do mocnych materiałów dowodowych. M.H. Baer wskazuje, że choć właściwą grupą docelową programu są aktualni lub byli pracownicy, to jednak istnieje jeden podstawowy element programu sygnalistów, który odstrasza ich od korzystania z tej ścieżki. Zgłoszenie informacji

---

110 *2018 Annual Report…*, s. 17.
111 J.P. Near, M.P. Niceli, *op. cit.*, s. 108.
112 M.H. Baer, *op. cit.*, s. 2217.

o przestępstwie i pomoc w skutecznym wyegzekwowaniu kar nie oznacza, że sam sygnalista nie zostanie skazany w postępowaniu karnym, jeśli okaże się, że w jakikolwiek sposób współdziałał w przestępstwie. Jest to o tyle ryzykowne, że stając się sygnalistą, wyjawia szczegóły dokonywanych działań, a także swoje nastawienie, np. to że był świadomy przestępczego charakteru działalności w mniejszym lub większym stopniu pomagał, etc. To znacznie ułatwia skazanie właśnie jego, gdyż organy ścigania i sąd nie muszą już martwić się o udowadnianie *mens rea*, które jest podstawą do przypisania większości przestępstw finansowych. W efekcie M.H. Baer uznaje, że w obecnym kształcie program sygnalistów może prowadzić do samooskarżenia. Przyciąga osoby przekonane o swojej niewinności, które jednak rzadko mają dostęp do mocnych materiałów dowodowych, a odstrasza osoby przekonane choćby o najdrobniejszym współudziale w przestępstwie[113].

W pewnej mierze o zasadności twierdzeń M.H. Baera przekonuje sam raport Komisji SEC. Informacje, które dostarczyli sygnaliści, były bardzo szczegółowe. Sygnaliści identyfikowali konkretne osoby zaangażowane w przestępstwa, dostarczali konkretne dokumenty, które uwiarygadniały zarzuty, informowali, gdzie takie dokumenty są przechowywane. Czasami identyfikowali konkretne operacje finansowe, które potwierdzały oszustwa albo pozwalały na bardziej precyzyjną kwalifikację naruszenia. Zazwyczaj informacje dotyczyły aktualnie dokonywanych naruszeń lub dopiero dokonanych. Ponadto niemal wszyscy sygnaliści dostarczali dodatkowe informacje, wyjaśnienia i dowody, już po fakcie zgłoszenia po raz pierwszy informacji o naruszeniach[114].

Istnienie wewnętrznych procedur zgłaszania naruszeń pozwala podmiotom działającym na rynku finansowym w zapobieganiu popełniania przestępstw. Wspomniane zagrożenie dla tych procedur może wynikać z wynagradzania zgłoszeń do zewnętrznego programu sygnalistów. W doktrynie wskazuje się, że wraz ze wzrostem nagrody, początkowo wzrasta także odsetek wewnętrznych zgłoszeń, jednakże po osiągnięciu pewnego maksimum korzystniej zgłaszać naruszenia tylko do zewnętrznego programu sygnalistów. Zatem ustanawiane nagrody nie mogą być ani zbyt małe, ani

[113] *Ibidem*, s. 2227, 2246, 2254, 2265, 2280.
[114] *2018 Annual Report…*, s. 16–17.

zbyt duże, tak aby po pierwsze zachęcić do zgłaszania informacji organom państwa, a po drugie nie zniechęcić do korzystania z wewnętrznych procedur w firmie[115]. Istotnym wyznacznikiem jest także rozwiązanie prawa amerykańskiego, które uzależnia możliwość zwiększenia nagrody od postawy sygnalisty w firmie: czy starał się wykorzystać wewnętrzne procedury kontrolne i zgłaszał naruszenia. Ponadto umożliwia otrzymanie przez niego nagrody, jeśli to sam zespół kontrolny zgłosi naruszenie lub wyniki kontroli do Komisji SEC, a oryginalna informacja pochodziła właśnie od tego sygnalisty. Wśród proponowanych zmian aktualnego Programu SEC Komisja uważa, że należy dać agencji możliwość bardziej elastycznego dostosowania wysokości nagrody tak, aby zachęcić przyszłych sygnalistów do korzystania z Programu[116].

Ostatnie informacje wskazują na dodatkowy słaby punkt programu SEC i CFTC[117]. Istnieje poważny problem z egzekwowaniem nałożonych przez obie agencje kar finansowych na podmioty naruszające prawo. Wpływa to bezpośrednio na wysokość nagród wypłacanych sygnalistom, a przede wszystkim na efektywność regulacji, która miała chronić rynek finansowy przed przestępczą działalnością. W 2018 r. agencja SEC wyegzekwowała tylko 28% z $ 4 000 000 000. Natomiast w ciągu ostatnich pięciu lat odsetek pobranych kar wyniósł 55% z $ 20 000 000 000. W ciągu pięciu pierwszych lat działania programu, tj. od 2009 r. odnotowano najwyższą średnią skuteczność – 60% z $14 600 000 000. Druga z agencji – CFTC – w 2018 r. miała rekordową skuteczność, tj. 90%, co dało $ 857 000 000 wpływów. Jednak CFTC nie upublicznia informacji o nałożonych karach, a podaje tylko coroczne wpływy z tych kar, co utrudnia weryfikację danych, które należności zostały w danym roku wyegzekwowane. Po pierwsze, problem tkwi w ograniczonych uprawnieniach obu agencji, jeśli chodzi o egzekucję kar z majątku dłużnika. Zgodnie z amerykańskim prawem SEC nie ma innych uprawnień niż prywatni wierzyciele, nie ma możliwości zajęcia majątku ani jego konfiskaty. Może tylko zgłaszać wnioski o ustanowienie zastawu na majątku dłużnika albo zgłaszać

---

[115] M. Iwasaki, *op. cit.*, s. 22–23.

[116] https://www.federalregister.gov/documents/2018/07/20/2018-14411/whistleblower-program-rules [dostęp: 9.05.2019].

[117] D. Michaels, *U.S. Fines Billions for Wall Street Fraud. Nearly Half the Time It Doesn't Collect*, „The Wall Street Journal", 20.05.2019, https://www.wsj.com/articles/some-securities-fraudsters-escape-paying-sec-fines-11558344601 [dostęp: 16.07.2019].

wnioski o wydanie nakazu wypełnienia wyroku sądu w obliczu bierności dłużnika. Sprowadza się to do toczenia długich procesów sądowych, szczególnie gdy nałożona kara dotyczy dużych podmiotów rynku finansowego. W związku z tym pojawia się drugi problem: opieszałość w obliczaniu zaległych należności oraz opóźnienia w ich dochodzeniu, a nawet spisywanie na straty tych, których nie udało się uzyskać w ciągu dwóch lat od nałożenia[118]. W celu usprawnienia systemu egzekwowania kar agencje starają się zatem poprawić swoją kulturę organizacyjną. Po pierwsze, zwiększają personel prawniczy odpowiedzialny za staranne dochodzenie zapłaty kar, a po drugie, pracują nad systemem komputerowym, który pozwoli ułatwić ustalenie, które kary jeszcze nie zostały zapłacone i jaka jest ich rzeczywista wysokość. Potwierdza się również w tym przypadku, że sama regulacja prawna nie jest wystarczająca, duże znaczenie mają: odpowiednie rozłożenie obowiązków, dobór właściwego zespołu pracowników oraz korzystanie z nowoczesnej technologii.

W doktrynie wskazuje się, że nie tylko właściwe ustalenie wysokości nagrody decyduje o korzystaniu z wewnętrznych procedur. Co do zasady, najpierw sygnaliści będą zgłaszali naruszenia wewnątrz firmy, ponieważ standard dowodu istnienia naruszenia jest wyższy w zewnętrznym programie sygnalistów niż w przypadku wewnętrznych procedur[119]. Sygnalista musi mieć czas, aby zebrać wystarczająco wiarygodny materiał, aby mógł ubiegać się o ochronę w ramach Programu. Czasami nie jest możliwe zebranie takich dowodów, a wówczas i tak pozostaje ścieżka wewnętrzna. Ponadto potrzeba istnienia wewnętrznych procedur, niezależnie od zewnętrznych programów sygnalistów, wynika z niepieniężnych motywacji do zgłaszania naruszeń: poczucia winy, poczucia obowiązku społecznego i odpowiedzialności społecznej.

Niemniej argumenty nie przekonują wszystkich: o ile USA i Kanada wprowadziły politykę nagradzania zewnętrznych sygnalistów, Wielka Brytania odrzuciła taki pomysł właśnie z obawy o zniechęcenie do korzystania z wewnętrznych procedur.

W doktrynie spotyka się propozycje, aby uzależnić zgłoszenie naruszenia do Komisji (SEC) od wykorzystania najpierw wewnętrznych procedur kontrolnych. Pozwoliłoby to na wykorzystanie w pełni stosowanych już bardzo

[118] *Ibidem*.
[119] M. Iwasaki, *op. cit.*, s. 9.

często wewnętrznych programów wykrywania naruszeń w podmiotach, do których utworzenia zobowiązują przepisy prawa.

Pewnym rozwiązaniem byłoby wprowadzenie jako reguły takiej procedury zgłaszania w pierwszej kolejności naruszeń wewnętrznym organom podmiotu. Natomiast należałoby umożliwić zgłaszanie naruszeń natychmiast do Programu zewnętrznego w wyjątkowych przypadkach, o których mówi sam Program, w sytuacji, gdy dopuszcza uczestniczenie w Programie osób na stanowiskach kierowniczych, a zatem:

- jeśli taka osoba ma uzasadnioną podstawę (*reasonable basis*), aby sądzić, że zgłoszenie informacji do Komisji jest konieczne w celu uniemożliwienia działań, które mogą bardzo prawdopodobnie wyrządzić poważną szkodę (*likely to cause substantial injury*) interesowi finansowemu podmiotu lub jego majątkowi lub jego inwestorom;
- jeśli taka osoba ma uzasadnioną podstawę (*reasonable basis*), aby sądzić, że podmiot, podejmuje działania, które doprowadzą do uniemożliwienia wykrycia dokonanego naruszenia;
- jeśli minęło co najmniej 120 dni od zgłoszenia przez taką osobę informacji o naruszeniu wewnątrz firmy właściwemu zespołowi, który zajmuje się audytem wewnętrznym, dyrektorowi działu prawnego, dyrektorowi komórki ds. *compliance* (lub odpowiednikowi), własnemu przełożonemu; albo jeśli minęło 120 dni od momentu, gdy ta osoba otrzymała informację o naruszeniu, i okoliczności wskazywały, że o tym naruszeniu wiedzą również zespół, który zajmuje się audytem wewnętrznym, dyrektor działu prawnego, dyrektor komórki ds. *compliance* (lub odpowiednik) lub własny przełożony.

Jednakże, nawet przy obecnej regulacji amerykańskiej, aż 83% z nagrodzonych sygnalistów korzystało z wewnętrznej procedury kontroli naruszeń. Pozytywny wpływ na ten odsetek z pewnością ma również wspomniana możliwość zmniejszenia nagrody, jeśli ktoś uniemożliwia lub opóźnia wewnętrzną kontrolę w firmie, która dotyczy zgłaszanych naruszeń. Niemniej, dużo zależy też od sposobu traktowania sygnalistów wewnątrz firmy. Istnienie programów zewnętrznych wymusza efektywny system *compliance* i wewnętrzny program sygnalistów. Wszak poziom standardów firmy będzie oceniany według liczby zewnętrznych zgłoszeń, im ich więcej, tym mniej zaufania i aktywności wewnętrznych struktur bezpieczeństwa. Warto zatem, aby pracodawcy starali

się ze zrozumieniem przyjmować sygnalistów. Eksperci w tym zakresie radzą, aby zapewnić wsparcie dla wewnętrznych sygnalistów, badać zgłoszone nadużycia i dzielić się wynikami z pracownikami, a przede wszystkim nie brać odwetu na sygnaliście, stosując np.: niskie oceny za wykonaną pracę; ścisłą kontrolę codziennych obowiązków; słowną krytykę czy reprymendę[120].

Z tego powodu w doktrynie amerykańskiej podnosi się, że wewnętrzny program sygnalistów jest środkiem prewencyjnym, który pozwala na zapobieganie naruszeniom. Natomiast zewnętrzny program sygnalistów pełni funkcję odstraszającą[121]. Właściwa wysokość nagród w programach zewnętrznych motywuje do korzystania ze środków wewnętrznych. Co więcej, pojawiają się głosy, że same firmy mogłyby rozważyć efektywność nagród w swoich wewnętrznych programach sygnalistów. Z pewnością obok korzyści finansowych najbardziej istotnym elementem jest tworzenie efektywnych środków ochrony sygnalistów wewnątrz instytucji, gdyż to jest kolejnym czynnikiem podnoszącym odsetek zgłaszanych naruszeń. Powyższy przykład rozwiązań amerykańskich mógłby być brany pod uwagę przy ocenie efektywności wprowadzanych obecnie regulacji chroniących sygnalistów, informujących o przestępstwach popełnianych w ramach działalności podmiotów zbiorowych[122].

Na potrzeby prawa polskiego warto także zwrócić uwagę na dwie propozycje, które pojawiły się w doktrynie prawa amerykańskiego oraz polskiego. Pierwsza, wskazana przez M.H. Baera, prowadzi do uwzględnienia w ewentualnym programie sygnalistów zwolnienia, redukcji lub odstąpienia od pociągania do odpowiedzialności karnej sygnalistów. Należy jednak pamiętać, że rozwiązanie to nie mogłoby być domyślne ani występować razem z nagrodą pieniężną. W innym wypadku mogłoby zaszkodzić funkcji odstraszającej prawa karnego, niwelując obawy przed angażowaniem się w działania wątpliwe prawnie. Ponadto, mogłoby doprowadzić do utożsamienia sygnalistów z przestępcami, którzy ostatecznie decydują się na współpracę, podczas gdy w opinii publicznej amerykańskiej pełnią raczej rolę quasi -bohaterów. Druga propozycja, wyrażona przez J. Polańskiego na gruncie

[120] J.P. Near, M.P. Miceli, *op. cit.*, s. 112.

[121] M. Iwasaki, *op. cit.*, s. 10–12.

[122] http://orka.sejm.gov.pl/Druki8ka.nsf/Projekty/8-020-1211-2019/$file/8-020--1211-2019.pdf [dostęp: 9.05.2019].

programów antymonopolistycznych, wskazuje, aby obok nagrody płaconej ze środków skutecznie odzyskanych przez organy państwowe wprowadzić pewną ryczałtową, niską sumę pieniężną płaconą na wcześniejszych etapach współpracy sygnalisty. Może to pozwolić na złagodzenie występujących już dolegliwości, a także zmotywować do dalszej współpracy w celu zniwelowania lub zapobieżenia przestępstwu.

Doświadczenie prawa amerykańskiego ukazuje różne modele kształtowania programu sygnalistów, a także wiążące się z nimi szanse oraz zagrożenia. Pomysł na zapewnienie udziału sygnalisty w wartości majątkowej odzyskanej przez państwo wydaje się dość uniwersalny. Swoimi korzeniami sięga prawa rzymskiego, w którym osoby zawiadamiające państwo o spadkach bezdziedzicznych, które miały przypadać skarbowi (*caducum*), mogły zatrzymywać najpierw połowę ich wartości, a następnie jedną czwartą[123]. Mogły tak czynić również osoby, które weszły w posiadanie tych dóbr pomimo braku zdolności do ich nabycia, a zatem ze świadomością, że dobra te podlegają reżimowi kaduku. Opamiętanie się i przyznanie skarbowi państwa tego, co mu się należy, również było przyjmowane z akceptacją. Dla Rzymian było to rozwiązanie bardzo pragmatyczne, pozwalało zaoszczędzić wydatki na administrację oraz kontrolowanie przestrzegania prawa. Dzisiaj program sygnalistów także uznawany jest za najtańszy dla państwa, choć o wiele trudniej jest ukształtować go w taki sposób, aby realnie dawał szansę na przerwanie spirali przestępstwa pojedynczym osobom.

2.7. Nowelizacja – art. 304 Kodeksu karnego (przeciwdziałanie nieetycznym operacjom pracowników instytucji finansowych)

Charakter zmian: nowelizacja obowiązujących aktów prawnych
Obszar zmian: Kodeks karny, Kodeks cywilny

Tezy:

1. Dodanie do znamion typu czynu zabronionego alternatywy dla wykorzystania przymusowego położenia – wykorzystanie niewiedzy albo

[123] Por. szerzej: G. Blicharz, *Udział państwa w spadku. Rzymska myśl prawna w perspektywie prawnoporównawczej*, Kraków 2016.

niedoświadczenia w celu przeciwdziałania pokusie nadużycia wykorzystującej asymetrię informacji.
2. Rozdzielenie przepisu ze względu na przedmiot ochrony (podmioty profesjonalne).
3. Doprecyzowanie przepisów Kodeksu cywilnego odnośnie do oprocentowania – odróżnienie oprocentowania od odsetek.

Proponowane brzmienie art. 304 Kodeksu karnego:

- Możliwość 1 (propozycja służąca wypracowaniu rozwiązań, z których mogą korzystać podmioty instytucjonalne)

§ 1 Kto, wyzyskując przymusowe położenie, niedołężność lub niedoświadczenie, zawiera z nią umowę, nakładając na nią obowiązek świadczenia niewspółmiernego ze świadczeniem wzajemnym, podlega karze pozbawienia wolności do lat 3.

§ 2 Kto, rażąco wyzyskując przymusowe położenie osoby prawnej albo jednostki organizacyjnej, niemającej osobowości prawnej, zawiera z nią umowę, nakładając na nią obowiązek świadczenia niewspółmiernego ze świadczeniem wzajemnym, podlega karze grzywny.

- Możliwość 2 (propozycja służąca wypracowaniu rozwiązań, z których mogą korzystać osoby fizyczne)

§ 1 Kto, wyzyskując przymusowe położenie, niedołężność lub niedoświadczenie, zawiera z nią umowę, nakładając na nią obowiązek świadczenia niewspółmiernego ze świadczeniem wzajemnym, podlega karze pozbawienia wolności do lat 3.

Uzasadnienie:

Celem tej nowelizacji jest wykorzystanie prewencyjnej i wychowawczej roli prawa karnego do skłonienia pracowników instytucji finansowych do przyjęcia służebnej roli względem swoich klientów w stosunku zobowiązaniowym. Zmiana optyki z opartej na jak największej prowizji sprzedażowej (będącej pochodną narzucanych pracownikom planów sprzedażowych instrumentów finansowych) na optykę zorientowaną na interes klienta wpłynie pozytywnie na obniżenie przestępczości pracowników instytucji finansowych.

Kwestią dyskusyjną jest kryminalizacja nieekwiwaletności świadczeń w stosunkach profesjonalnych. Pozostawia to bowiem mniejszą swobodę

działalności gospodarczej zarówno instytucjom finansowym, jak i ich klientom. Można bowiem wyobrazić sobie sytuację, w której z powodu ogromnych problemów z płynnością finansową przedsiębiorstwo decyduje się na wzięcie kredytu, a następnie po nieudanej próbie wyjścia z problemów finansowych zgłasza do organów ścigania możliwość popełnienia przestępstwa przez pracownika instytucji finansowej, który rzekomo wykorzystał jej przymusowe położenie i zaproponował cenę kredytu nieekwiwalentną do poniesionego przez instytucję ryzyka.

Wydaje się raczej, że przepis ten pierwotnie miał na celu ochronę osób fizycznych[124] przed popadaniem w spiralę długów, którą ich wierzyciele mogliby wykorzystać do zrobienia sobie ze swoich dłużników „ekonomicznych niewolników". W parze z częściowo zliberalizowaną wersją tego przepisu (chodzi o część dotyczącą podmiotów profesjonalnych) należałoby się pochylić nad kwestią oprocentowania maksymalnego, tak by instytucje finansowe w ryzykownych przedsięwzięciach nie musiały ukrywać swoich kosztów ryzyka w ogromnej liczbie kosztów pobocznych kredytów.

Zjawisko wykorzystywania asymetrii informacji przez pracowników instytucji finansowych i pokusa nadużycia stanowiły walny fundament nieprawidłowości w prywatnym sektorze finansowym, zarówno w Europie, jak i na innych kontynentach po okresie deregulacji sektora finansowego lat 80. XX wieku[125]. Można było dostrzec zmianę podejścia do klientów instytucji finansowych ze służebnej na zorientowaną na indywidualny zysk pośrednika. To skłoniło prawodawców do powrotnego uregulowania tego sektora gospodarki, z tym jednak, że przepisy skupiły się głównie na prawie prywatnym.

Nietrudno w ostatnich kilku latach znaleźć przykłady działalności pracowników instytucji finansowych w Polsce, które pasują do zarysowanego wyżej opisu. Mowa na przykład o zjawisku sprzedawania „polisolokat", które nie dawały klientom praktycznie żadnych szans na zarobek[126], a znajdywały swoich nabywców właśnie przez wykorzystanie niewiedzy finansowej lub

---

[124] W. Zalewski, *Lichwa*, [w:] *System prawa karnego*, red. R. Zawłocki, Warszawa 2015, s. 737.

[125] J. Kulawik, *Deregulacja systemów bankowych w wybranych krajach*, „Bank i Kredyt" 2003, nr 8.

[126] Jest to teza pochodząca z raportu Rzecznika Finansowego, https://rf.gov.pl/pdf/RAPORT%20UFK-CZ%202-WERSJA%20OST-30-03-2016%20pop.pdf [dostęp: 10.05.2019].

niedoświadczenia czy sprzedawaniu opcji walutowych o ogromnej dźwigni finansowej nieświadomym przedsiębiorcom nieświadomych klientów czy o kredytach indeksowanych bądź denominowanych w walutach obcych. Taka asymetria informacyjna dotknęła też przecież profesjonalne podmioty, które w 2008 roku padły ofiarą toksycznych opcji walutowych, które doprowadziły wiele firm niemalże do bankructwa, ze względu na przyjętą dźwignię finansową. W tych okolicznościach trudno zarzucić prawnie cokolwiek pracownikom banku, którzy oferowali takie instrumenty finansowe osobom nieposiadającym wystarczającej wiedzy finansowej. Wszak same wyraziły zgodę na zakup takich usług. Można jednak dostrzec dysonans na płaszczyźnie etycznej, bo przecież stosunki zobowiązaniowe, których stroną są instytucje finansowe, mają służyć zwiększeniu efektywności gospodarki (nie wyłączając, rzecz jasna, tytułu takich podmiotów do wynagrodzenia za takie usługi) i są oparte na zaufaniu klientów do usług świadczonych przez te podmioty.

Jedynym instrumentem, który jest odpowiedzią na nadmierne wykorzystywanie asymetrii informacji w stosunkach zobowiązaniowych, jest art. 388 Kodeksu cywilnego, który pozwala na dostosowanie nieekwiwalentnego świadczenia wzajemnego albo unieważnienie umowy, gdy powstała ona w warunkach wykorzystania przez jedną stronę przymusowego położenia, niedołęstwa albo niedoświadczenia drugiej strony. O ile Kodeks karny kryminalizuje wyzyskanie przymusowego położenia innej osoby fizycznej, prawnej albo jednostki organizacyjnej niemającej osobowości prawnej w drodze zawarcia umowy, nakładającej na wykorzystaną stronę obowiązek świadczenia niewspółmiernego ze świadczeniem wzajemnym, to trudno znaleźć tam reakcję prawodawcy na naruszenie stosunku zaufania i wykorzystanie asymetrii informacji w relacji prawnej klienta i instytucji finansowej w drodze wykorzystania niedołęstwa albo niedoświadczenia drugiej strony, a przecież wskazane powyżej społecznie nieakceptowalne zachowania można tak zakwalifikować. W piśmiennictwie podkreśla się subsydiarny charakter art. 304 Kodeksu karnego względem art. 388 Kodeksu cywilnego. Z tej ścisłej relacji nie można jednak wywieść, że wykorzystanie niedołęstwa i niedoświadczenia drugiej strony stanowi znamię typu czynu zabronionego.

Zaproponowane wyżej rozwiązanie polegające na dołączeniu dodatkowych okoliczności, w których występuje wyzysk, przewiduje niemiecki Kodeks karny. Do okoliczności, w których zachodzi do zastrzeżenia nieekwiwalentnych

świadczeń, zalicza się w nim: trudną sytuację, niedoświadczenie, niezdolność do właściwego osądu oraz słabość woli. Zgodnie z niemieckim prawem kryminalnym brak rozeznania, a w konsekwencji niedoświadczenie, nie mogą być jednak okolicznościami uzasadniającymi przypisanie odpowiedzialności karnej, jeżeli zainteresowany nie zapoznał się z ofertą innych banków, zatem nie dochował należytej staranności[127]. Jeżeli zaś chodzi o niezdolność w rozpoznawaniu okoliczności, który może być podstawą odpowiedzialności karnej, to może mieć on charakter przejściowy, ale powinien skutkować niemożnością kierowania się racjonalnymi pobudkami ocenienia wzajemnych wyników i konsekwencji ekonomicznych[128]. Ponadto, przepis ten chroni interesy gospodarcze podmiotów nieprofesjonalnych. Jest to szczególny przypadek – Kodeksy karne krajów europejskich czy konkretnych stanów Kanady czy Stanów Zjednoczonych Ameryki Północnej w przepisach nawiązujących do wykorzystania niedoświadczenia czy niedołęstwa nie zawierają szczególnego przepisu dotyczącego nieekwiwaletności świadczeń.

Oczywiście należy w tym miejscu poczynić uwagę dotyczącą różnego charakteru podmiotów będących klientami instytucji finansowych. Od przedsiębiorców wymaga się większej staranności w prowadzonej przez siebie działalności i trudno objąć ich taką samą ochroną prawną jak konsumentów. Z tego też powodu przepis ten, oprócz dodatkowych, alternatywnych znamion powinien zostać rozdzielony, tak by zagwarantować zróżnicowany standard ochrony ze względu na charakter przedmiotu ochrony (nieprofesjonalni i profesjonalni uczestnicy obrotu). Stąd należy dodać do przepisu odnoszącego się do podmiotów profesjonalnych sformułowanie wartościujące „rażąco wykorzystuje", tak by wyłącznie kwalifikowane wykorzystywanie przymusowego położenia było podstawą odpowiedzialności karnej. W przypadku podmiotów tego rodzaju należałoby pominąć znamię niedołęstwa, jest właściwe dla nieprofesjonalnych uczestników obrotu.

Dla spójności znamion typu czynu zabronionego, które pozostawałyby w jeszcze silniejszej relacji z art. 388 k.c. należałoby też doprecyzować regulację oprocentowania, które znajduje się w Kodeksie cywilnym, tak by ograniczyć

[127] Schmidt BeckOK StGB, v. Heintschel-Heinegg, 40. Edition (StGB § 291 Wucher, Rn. 25).

[128] Münchener Kommentar zum StGB (StGB § 291 Wucher, Rn. 18).

prawdopodobieństwo błędnego zakwalifikowania działalności pracowników instytucji finansowej jako kryminalizowany wyzysk. Należy wyrazić dopuszczalność pobierania odsetek karnych od wynagrodzenia pieniężnego za usługi kredytowe (oprocentowanie), gdyż dotychczasowe brzmienie przepisów dotyczących odsetek (zakaz anatocyzmu), z powodu niespójności terminologicznej budzi niepotrzebne wątpliwości. Jeżeli chodzi zaś o regulację wysokości oprocentowania i odsetek w stosunkach konsumenckich, polski porządek prawny jest w tej mierze spójny i jasny. W tej części dla koherencji z proponowaną nowelizacją nie ma potrzeby jakiejkolwiek ingerencji.

Choć zarysowana wyżej nowelizacja jest raczej elementem następczej kontroli operacji pracowniczych, to spełnia też rolę bodźca wpływającego motywacyjnie na pracowników instytucji finansowych[129]. Wykorzystywanie asymetrii informacyjnej to bowiem plaga społeczeństwa informacyjnego, które staje się zjawiskiem globalnym. Fiducjarny i misyjny charakter działalności instytucji finansowych nie może być oparty na mentalności sprzedażowej. Przeciwdziałanie przestępczości musi wiązać się nie tylko z procedurami kontrolnymi i reagowaniem na nieprawidłowości. Jego nieodzownym elementem musi też być korygowanie etyczne. Wychowawcza rola prawa karnego połączona ze skutecznymi mechanizmami kontroli działalności operacyjnej instytucji finansowych realizowanych przez ich pracowników zdaje się spójną strategią prewencyjną dla prywatnego sektora finansowego.

[129] K. Jadach, *Wymiar sprawiedliwości w kontekście zakładanych funkcji kary*, „Studia Edukacyjne" 2013, nr 23, s. 187.

ROZDZIAŁ TRZECI

Analiza procesu podejmowania decyzji w instytucjach finansowych

Proces podjęcia decyzji można zdefiniować jako dokonanie wyboru jednej z co najmniej dwóch możliwości. Zakładając racjonalność podmiotu podejmującego decyzję, należy przyjąć, że wybór dotyczy sposobu realizacji przyjętego przez podmiot celu[130].

Proces decyzyjny obejmuje grupę powiązanych operacji myślowych, uporządkowaną, umożliwiającą zarówno ocenę sytuacji decyzyjnej, jak i wybór najkorzystniejszego wariantu[131]. Czynnikiem odpowiedzialnym za rozpoczęcie procedury podejmowania decyzji jest sytuacja problemowa. Z koniecznością dokonania wyboru określonego działania mamy do czynienia w takich sytuacjach, w których interwencja menedżera jest niezbędna lub możliwe jest wskazanie naraz wielu alternatywnych sposobów interwencji. Interwencja menedżerska wiąże się zazwyczaj z wprowadzeniem zmian wewnątrz organizacji lub w jej otoczeniu. Osoba wypełniająca obowiązki menedżera jest zobowiązana do dokonania wyboru rozwiązania, gdy występujące lub mające wystąpić zagrożenia wymagają zamiany istniejącego, niekorzystnego stanu rzeczy na satysfakcjonujący lub niedopuszczenia do stanu niepożądanego[132]. Podjęcie decyzji jest konieczne również w wypadku, gdy organizacja staje przed wyborem jednego lub więcej spośród różnorodnych, pożądanych i niemożliwych do jednoczesnego zrealizowania celów, a także gdy należy wybrać środki realizacji tych celów oraz rozłożyć ciężar zysków i strat związanych z ich

[130] J. Penc, *Decyzje w zarządzaniu*, Kraków 1995.

[131] K. Klincewicz, *Zarządzanie, organizacje i organizowanie – przegląd perspektyw teoretycznych*, Warszawa 2016.

[132] K. Bolesta-Kukułka, *Decyzje menedżerskie w teorii i praktyce zarządzania*, Warszawa 2003.

realizacją. Wśród zdarzeń rozpoczynających proces podejmowania decyzji można zatem wskazać przyczyny reaktywne (odnoszące się do zaistniałych zdarzeń) i proaktywne (wyprzedzające lub kreujące przyszłe zdarzenia).

Sam akt podjęcia decyzji jest końcowym etapem wspomnianego już procesu decyzyjnego utożsamianego przez niektórych z procesem zarządzania projektami instytucji finansowej i rozumianego właśnie jako sekwencyjny, przemyślany proces podejmowania decyzji dotyczących wszystkich zasobów projektu[133]. W ramach procesu decyzyjnego możliwe jest wskazanie ośmiu etapów[134]:

1. Identyfikacja i formułowanie problemu decyzyjnego,
2. Identyfikowanie kryteriów wyboru wariantu decyzyjnego,
3. Przypisanie wag do poszczególnych kryteriów wyboru (gdy korzystamy z kilku),
4. Opracowanie wariantów decyzyjnych,
5. Analiza wariantów decyzyjnych według wcześniej określonych kryteriów,
6. Wybór wariantu (podjęcie decyzji),
7. Wdrożenie wybranego wariantu,
8. Kontrola, ocena realizacji oraz ewentualne korekty działania.

Podmiot podejmujący decyzje najczęściej nie jest w stanie ustalić wszystkich faktów mających wpływ na sytuację, w związku z którą zmuszony jest dokonać wyboru. Zdecydowana większość decyzji podejmowanych i realizowanych przez instytucje finansowe zapada zatem w stanie niepełnej wiedzy, co w doktrynie określa się mianem racjonalności ograniczonej[135].

Ze względu na fakt, że głównym celem podmiotów sektora prywatnego działających na rynku finansowym jest osiąganie zysków, znaczny nacisk kładziony jest na ogół na posiadanie przez osoby decyzyjne stosownych kompetencji oraz na działanie w oparciu o procedurę pozwalającą uniknąć najgorszych błędów w ocenie sytuacji. Trafność decyzji ma wpływ na wyniki ekonomiczne danej instytucji. Trafne decyzje służą osiąganiu zysku i unikaniu straty, natomiast decyzje błędne przeciwnie – prowadzą do strat. W trosce

[133] W. Walczak, *Rola fazy planowania w zarządzaniu projektami*, „E-mentor" 2010, nr 1(33).

[134] K. Bolesta-Kukułka, *op. cit.*

[135] *Ibidem.*

o trwałe zwiększenie jakości podejmowanych decyzji formułowane są różne przesłanki mające zwiększać szanse na podjęcie trafnej decyzji niezależnie od poziomu posiadanych przez decydenta kompetencji[136]. Wśród nich wymienić należy precyzyjne zdefiniowanie problemu, określenie czynników korzystnych dla organizacji, opracowanie planów działania, odpowiedzialność za decyzje, odpowiedzialność za komunikację, zwiększoną koncentrację na możliwościach zamiast problemach, produktywne zebrania oraz koncentrację na „my" zamiast „ja". Precyzyjne określenie wyzwania stojącego przed instytucją oraz opisanie wszystkich czynników, mogących mieć wpływ na jej sytuację, wydaje się niezbędnym minimum koniecznym dla wypracowania kompletnego i efektywnego rozwiązania pojawiającego się problemu. Równie istotne dla efektywności procesu decyzyjnego jest określenie celów, które zamierza zrealizować instytucja, oraz uwzględnianie ich przy podejmowaniu jakichkolwiek działań przez jej organy. Dopiero zestawienie tych dwóch stanów: stanu obecnego oraz stanu postulowanego (po zrealizowaniu konkretnych zadań) pozwala, w wyniku swoistej subsumpcji, dostrzec ogólne kierunki działań prowadzących do osiągnięcia założonego celu. Należy podkreślić, że ustalenie ogólnych kierunków działania w połączeniu z wykształceniem platformy komunikacji i weryfikacji proponowanych, konkretnych rozwiązań, służyć powinno przygotowaniu planów realizacji przyjętych przez instytucję zadań i priorytetów. Wcześniejsze planowanie umożliwia bowiem instytucjom uporządkowaną i efektywną reakcję oraz służy ograniczeniu strat, które mogłyby zostać wywołane błędnymi wyborami dokonanymi przez nieprzygotowanych decydentów.

Analizując sposoby podejmowania decyzji w instytucjach finansowych, można wyróżnić cechy wspólne wszystkich metod dokonywania wyboru (tabela poniżej).

[136] P.F. Drucker, *What Makes an Effective Executive*, „Harvard Business Review" 2004, no. 6.

Tabela 1. Cechy wspólne metod dokonywania wyboru w instytucjach finansowych.

	Poszukiwanie	Synteza	Analiza
Formułowanie problemu			
Konceptualizacja rozwiązań			
Uszczegółowienie			
Ocena/Ewaluacja			
Wdrożenie			

Źródło: opracowanie własne na podstawie P. Nutt, *Types of Organizational Decision Processes*, „Administrative Science Quaterly" 1984, vol. 29, s. 414–450.

Przez formułowanie problemu rozumie się na ogół podjęcie działań zmierzających do poznania problemu oraz powodów jego wystąpienia, równolegle z przeanalizowaniem potrzeb i możliwości instytucji. Faza konceptualizacji natomiast oznacza zaproponowanie rozwiązań umożliwiających realizację celów instytucji. Etap uszczegółowienia polega zaś na dopracowaniu zaproponowanego wcześniej rozwiązania, tak aby było ono wykonalne. Podczas ewaluacji rozwiązań ocenia się ich koszty i korzyści. Po dokonaniu oceny następuje wybór jednej z opcji oraz jej wdrożenie. Wskazane pięć etapów podejmowania decyzji należy przyporządkować do wskazanych w powyższej tabeli czynności poszukiwania, syntezy oraz analizy. Poszukiwania polegają na zgromadzeniu informacji. Podczas syntezy rozpatruje się związki pomiędzy zgromadzonymi informacjami. Analiza natomiast zmierza do wydania osądu na temat posiadanych danych.

W literaturze przedmiotu pojawiają się jednak również inne propozycje opisania procesu decyzyjnego[137]. Badania skupiają się na ogół na uzyskaniu odpowiedzi na dwa zasadnicze pytania: jak powinny być podejmowane decyzje? jak wygląda proces podejmowania decyzji? Udzielając odpowiedzi na pierwsze z przedstawionych pytań, należy wskazać zestaw norm i zasad procesu decyzyjnego (czyli tzw. normatywne, inaczej, preskryptywne modele podejmowania decyzji), jeżeli zaś chodzi o drugie z zadanych pytań, to chodzi o opisy przebiegu rzeczywistych procesów podejmowania decyzji (deskryptywne, inaczej: opisowo-wyjaśniające modele podejmowania decyzji)[138].

[137] K. Klincewicz, *op. cit.*
[138] *Ibidem.*

Założeniem stojącym u podstaw metod normatywnych jest przekonanie, że człowiek działa racjonalnie, w związku z czym odkrycie trafnego, spójnego algorytmu nieuchronnie prowadzi do najlepszego w kontekście przyjętego kryterium rozwiązania. Preskryptywne modele decyzyjne charakteryzują się dedukcyjnością przyjętego rozumowania, polegającą na przejściu od założeń abstrakcyjnych do szczegółowych prawidłowości, wreszcie zaś do konkretnych sposobów postępowania[139]. Modele preskryptywne zostały poddane analizie w poniższej tabeli.

Tabela 2. Perspektywne modele decyzyjne.

Model	Opis
Altmana, Valenziego i Hodgettsa (monokryterialny) (Bolesta-Kukułka, 2000, s. 42)	Etapy procesu decyzyjnego: 1. Odkrycie trudności 2. Zidentyfikowanie specyficznego problemu 3. Określenie kryterium oceny wariantów decyzyjnych 4. Zestawienie listy rozwiązań 5. Określenie efektów zastosowania każdego rozwiązania 6. Wybór najlepszego wariantu 7. Wdrożenie decyzji Punktem wyjścia typologii decydentów jest psychologiczna metoda C.G. Junga, według której osobowość każdego człowieka jest zdominowana przez jedną z funkcji: doświadczenie, myślenie, intuicję, emocje. Opierając się na niej, wyodrębnili następujące typy decydentów: empirysta, intelektualista, intuicjonista, uczuciowiec.
Robbinsa i Coulter (wielokryterialny) *Decyzje menedżerskie w teorii i praktyce zarządzania*, red. K. Bolesta-Kukułka, Warszawa 2000. (Dalej: Bolesta-Kukułka, 2000, s. 44)	Etapy procesu decyzyjnego: 1. Identyfikacja problemu 2. Identyfikacja kryteriów decyzyjnych 3. Przypisanie wag kryteriom 4. Opracowanie alternatyw 5. Analiza alternatyw 6. Selekcja (wybór) 7 Wdrożenie wybranego wariantu 8. Ocena efektywności decyzji Punktem wyjścia procesu decyzyjnego jest problem decyzyjny. Wybierana jest ta alternatywa, której użyteczność jest największa.

[139] *Ibidem.*

Model	Opis
Sutherlanda (Bolesta-Kukułka, 2000, s. 46)	Etapy procesu decyzyjnego: 1. Konieczność podjęcia decyzji (cel) 2. Informacje *a priori* (obecne opinie, teorie, sądy) 3. Informacje *a posteriori* (badania empiryczne) 4. Budowanie modelu 5. Generowanie rozwiązań 6. Wybór kryteriów oceny 7. Ocena wariantów 8. Wybór 9. Podjęcie decyzji 10. Wdrożenie 11. Sprzężenie zwrotne do korekty modelu Punkt wyjścia dla procesu decyzyjnego stanowią cel, sytuacja lub kontekst. Do realizacji przyjmowany jest wariant o najwyższej użyteczności.
Holta (Bolesta-Kukułka, 2000, s. 47)	Etapy procesu decyzyjnego: 1. Diagnoza problemu 2. Analiza otoczenia 3. Sformułowanie problemu 4. Opracowanie rozwiązań 5. Ocena wariantów 6. Wybór 7. Wdrożenie 8. Ocena efektów
Prakseologiczny (Redziak, 2013, s. 115)	Wybór najlepszej decyzji na podstawie kryterium sprawności. Decyzja optymalna jest skuteczna i ekonomiczna.
Badań operacyjnych (Redziak, 2013, s. 117)	Etapy procesu decyzyjnego: 1. Budowanie modelu (opisanie problemu językiem matematycznym) 2. Rozwiązanie – odszukanie optymalnej decyzji 3. Weryfikacja modelu – ewentualna poprawa 4. Kontrolowanie – informacja zwrotna oraz ewentualna korekta podjętej decyzji Badania operacyjne umożliwiają analizę wybranego obszaru rzeczywistości i prognozowanie – dokonanie oceny ilościowej możliwych rezultatów podjętej decyzji.
Cybernetyczny (Redziak, 2013, s. 122)	Etapy procesu decyzyjnego: 1. Wejście – informacja pierwotna, nieprzetworzona 2. Transformacja – proces decyzyjny 3. Wyjście – informacja wtórna w postaci decyzji Model znajduje się w otoczeniu, które bezpośrednio lub pośrednio wpływa na proces decyzyjny. Model opiera się na analogiach pomiędzy zasadami działania organizmów żywych, układów społecznych i maszyn.
Rozmytych reguł decyzyjnych (Redziak, 2013, s. 124)	Model bazuje na dwóch wartościach *1* (prawda) i *0* (fałsz), przy jednoczesnym założeniu, że podział na te wartości nie jest niezmienny i jednoznacznie określony. Pomiędzy stanem „prawda" a stanem „fałsz" jest szereg wartości pośrednich, a granice między nimi są rozmyte (np. „w dużej mierze to prawda", „wartość około 5")

Źródło: opracowanie własne na podstawie: *Decyzje menedżerskie w teorii i praktyce zarządzania*, red. K. Bolesta-Kukułka, Warszawa 2000; Z. Redziak, *Podstawy teorii podejmowania decyzji*, Warszawa 2013.

Zauważyć należy, że modele preskryptywne nie są w stanie dostarczyć rozwiązań wszystkich problemów napotykanych przez instytucje finansowe. Czynników praktycznie uniemożliwiających bowiem korzystanie

z reguł, sformułowanych w ramach tych metod, nie brakuje. Czynniki te należy podzielić na subiektywne, czyli zależnie od osób podejmujących decyzje (tutaj można wskazać brak kwalifikacji, umiejętności, doświadczenia lub negatywne cechy osobowości), a także czynniki obiektywne, wynikające z uwarunkowań zewnętrznych i wewnętrznych w danej instytucji finansowej. Modele preskryptywne odznaczają się brakiem elastyczności, stosowaniem zbytnich uproszczeń, a czasem też nieprzystawalnością zaleceń do rzeczywistych zachowań kierowników. Modele podejmowania decyzji są niezwykle rygorystyczne, a ich stosowanie często przekracza kompetencje menedżerów[140].

Mając na uwadze wymienione niedoskonałości modeli normatywnych, wskazać należy inne, pozbawione wad tych pierwszych, sposoby ukształtowania procesu decyzyjnego. Będą to tzw. metody deskryptywne, inaczej: opisowo-wyjaśniające lub behawioralne. Podobnie jak w przypadku metod normatywnych, tak i w przypadku metod deskryptywnych u podstaw procesu decyzyjnego leżą dwa precyzyjne pytania: jak w rzeczywistości podejmowane są decyzje i z jakiego powodu procesy decyzyjne wyglądają właśnie tak. Odwrotnie niż w poprzedniej grupie metod stosuje się tu na ogół metodę indukcyjną dochodzenia do wniosków (badanie pojedynczych przypadków prowadzić ma do wniosków abstrakcyjnych) w celu opisania i wyjaśnienia rzeczywistych procesów decyzyjnych.

Metody behawioralne podejmowania decyzji można podzielić na modele wspomnianej już racjonalności ograniczonej (za przykład może tu posłużyć model suboptymalizacji Simona[141]) oraz modele heurystyczne (np. model „kosza na śmieci"). Modele racjonalności ograniczonej uwzględniają w swej analizie procesu decyzyjnego ograniczenia wynikające z niedoskonałości ludzkich zdolności poznawczych. Modele heurystyczne charakteryzuje natomiast odejście od zasad i norm racjonalnego działania celem stymulowania kreatywności[142].

Model suboptymalizacji Simona wyraża głęboki sceptycyzm wobec propagowanych przez ekonomistów, preskryptywnych metod uporządkowania

---

[140] K. Bolesta-Kukułka, *op. cit.*

[141] H.A. Simon, *A Behavioral Model of Rational Choice*, „The Quarterly Journal of Economics" 1955, vol. 69, no. 1.

[142] Z. Redziak, *Podstawy teorii podejmowania decyzji*, Warszawa 2013.

procesu podejmowania decyzji[143]. Simon poddaje zdecydowanej krytyce koncepcję człowieka ekonomicznego (łac. *homo oeconomicus*, ang. *economic man*) jako istoty podporządkowanej we wszystkich swych działaniach nadrzędnej zasadzie maksymalizacji użyteczności. Zdaniem badacza pogląd ten jest bezpodstawny. W kontrze do wskazanej koncepcji Simon zaproponował teorię *homo satisfaciendus* – człowieka jako istoty dążącej do osiągnięcia zadowalającego minimum, wybierającej odpowiedzi i rozwiązania najmniej skomplikowane, a przy tym spełniające wszystkie stawiane przed nimi wymagania. Człowiek w opinii Simona świadomie lub nieświadomie rezygnuje z dalszych poszukiwań, mimo że mogłyby one doprowadzić do jeszcze lepszych rezultatów w momencie, w którym odnajdzie najprostsze, najmniej wymagające rozwiązanie. Ograniczona racjonalność (ang. *bounded rationality*) zdaniem Simona sprowadza się do rozważania ograniczeń, które związane są nierozłącznie z podejmowaniem decyzji. W rzeczywistości bowiem decydenci bardzo często znajdują się w sytuacji, gdy zmuszeni są wybierać rozwiązania w oparciu o niepełną wiedzę na temat rozwiązań alternatywnych i oraz możliwych konsekwencji swoich wyborów. Zauważyć należy, że nawet znajmość koniecznych danych nie gwarantuje podjęcia trafnej decyzji. Umysł ludzki posiada bowiem ograniczoną zdolność analizowania, rozumienia i zapamiętywania[144]. Przeszkody te, będące wynikiem zawodności ludzkich zdolności poznawczych, określa się mianem „poznawczych ograniczeń racjonalności"[145].

Należy zauważyć, że jednostka[146] dąży na ogół do realizacji wielu celów naraz oraz że cele te niekoniecznie są ze sobą zbieżne. Ze względu na brak pełnej wiedzy o wszystkich rozwiązaniach możliwych do zastosowania w związku z danym zdarzeniem problematycznym oraz ze względu na ograniczenia intelektualne, jednostka poszukuje na ogół rozwiązań najprostszych. W związku z wymienionymi cechami ludzkiego poznania należy uznać, że decydent nie kieruje się tak naprawdę zasadą optymalizacji – nie dąży bowiem w rzeczywistości do wyboru najlepszego z możliwych rozwiązań. Decydenci na ogół pozostają przy swojej pierwszej decyzji, o ile tylko zaspokaja ona ich oczekiwania. Przeszkodę tę, wynikającą po części z ludzkiej natury, określa

143 H.A. Simon, *Models of Man, Social and Rational*, Oxford 1957.
144 *Ibidem.*
145 K. Bolesta-Kukułka, *op. cit.*
146 H.A. Simon, *Models of Man*…

się mianem motywacyjnego ograniczenia racjonalności[147]. Odkrycie wystarczająco zadowalającego, będącego kompletną odpowiedzią na powstałe wątpliwości, rozwiązania kończy proces decyzyjny, gdyż brakuje motywacji do dalszej analizy alternatyw.

Niezwykle istotnym zagadnieniem w kontekście procesu decyzyjnego jest tzw. reguła zatrzymania (ang. *stop rule*). Mając na uwadze, że w rzeczywistości decydent nie posiada w jednym momencie wiedzy na temat wszystkich możliwych rozwiązań danego problemu, reguła zatrzymania mówi, w którym momencie należy przerwać proces poszukiwania rozwiązań celem podjęcia decyzji. Ponieważ nie jest możliwe zagwarantowanie, że decydent będzie miał w tym momencie wiedzę na temat najefektywniejszego rozwiązania, należy ustalić, jaki poziom realizacji potrzeby będzie satysfakcjonujący oraz doprowadzi do przerwy w poszukiwaniu alternatywnych rozwiązań. Wydaje się, że poziom zaspokojenia potrzeby jest proporcjonalny do szansy na odnalezienie rozwiązania zapewniającego osiągnięcie zamierzonych pozytywnych skutków decyzji. Wymagania dotyczące poziomu zaspokojenia rosną, gdy szansa na odnalezienie najefektywniejszego rozwiązania jest duża oraz maleją wraz z maleniem szansy[148]. Sformułowaną regułę określamy mianem „poszukiwania satysfakcjonującego rozwiązania" (ang. *satisficing*).

Należy zauważyć, że polski termin „wybór satysfakcjonujący" nie odzwierciedla pełnego znaczenia przymiotnika *satisficing* czy czasownika *to satisfice*. Oznaczają one nie tyle kompletne rozwiązanie, lecz takie, które pozwala w minimalnym, pozwalającym uniknąć strat stopniu poradzić sobie ze zdarzeniem problematycznym. Nie chodzi tu zatem wcale o rozwiązanie budzące pełnię zadowolenia. Zastosowanie tego modelu procesu decyzyjnego w skali całej organizacji oznacza ni mniej, ni więcej jak rozwiązywanie wielu problemów organizacyjnych poprzez poszukiwanie ekonomicznych, tanich i odpowiednich do osiągnięcia zamierzonego celu rozwiązań[149].

Kolejnym przykładem opisowo-wyjaśniającego modelu jest metoda tzw. „kosza na śmieci"[150]. Omawiany model zakłada brak racjonalności

---

147 K. Bolesta-Kukułka, *op. cit.*

148 H.A. Simon, *Models of Man…*

149 *Zarządzanie firmą. Strategie, struktury, decyzje, tożsamość*, oprac. Strategor [pseud. zbiorowy], Warszawa 1999.

150 J. Supernat, *Racjonalność i logika decyzji administracji*, Warszawa 2008.

w procesie podejmowania decyzji w instytucjach. Podmioty gospodarcze, jako „zorganizowane anarchie", są niezdolne do wypracowania spójnych celów i wartości. Przyjęty w nich proces decyzyjny jest niejasny i podlega częstym zmianom. Organizacje zbiorowe są na ogół słabo sformalizowane i nie posiadają opracowanych katalogów wewnętrznych reguł postępowania. Sami pracownicy instytucji często nie rozumieją bądź nie znają tych zasad, co w połączeniu z brakiem kanałów komunikacyjnych między nimi a jednostkami organizacyjnymi wewnątrz struktury instytucji sprawia, że proces podejmowania decyzji jest niezwykle chaotyczny. Proces podejmowania decyzji w omówionych warunkach zrównuje się właśnie z koszem na śmieci, w którym rozwiązanie problemu jest dziełem czystego przypadku i wypadkową działań niepowiązanych ze sobą zdarzeń i ludzi. Zdarzają się nawet, wcale nie tak zabawne, sytuacje, gdy decyzje poprzedzają stwierdzenie zaistnienia lub możliwości zaistnienia problemu[151]. Dodatkowym obciążeniem w procesach decyzyjnych jest wewnętrzna aktywność społeczno-polityczna osób współodpowiedzialnych za poszukiwanie rozwiązań. Nierzadko dochodzi bowiem tu do konfliktów na tym tle pomiędzy interesariuszami w instytucjach finansowych. Sytuacja decyzyjna może być problemem, okazją do decydowania, ale też znalezieniem zastosowania dla któregoś ze znajdujących się w „koszu" rozwiązań[152].

Najbardziej oryginalny wydaje się sposób patrzenia na procesy decyzyjne przyjęty przez model irracjonalny. Fundamentalnym elementem działalności menedżera, w tym ujęciu, nie jest wcale podjęcie decyzji, lecz efektywne działanie. Zdarza się bowiem, że na podstawie racjonalnych decyzji nie są podejmowane udane działania[153]. Dla efektywnego działania instytucji konieczne jest odpowiednie wdrażanie decyzji, w tym prezentowanie pozytywnego stosunku do własnych działań. Nie brakuje głosów, że racjonalny proces podejmowania decyzji wpływa niekorzystnie na motywację i gotowość do działania[154]. Ze względu na niespójność przyjętych celów racjonalny proces decyzyjny może wywoływać zwątpienie i niepewność. Analiza skutków dokonanego wyboru służy w takich wypadkach sianiu zwątpienia i niepewności,

---

151 *Ibidem.*
152 *Ibidem.*
153 M.J. Hatch, *Teoria organizacji*, Warszawa 2002.
154 *Ibidem.*

co dramatycznie obniża motywację i gotowość do działania. W tym wypadku odwołanie się do ustalonych racjonalnych kryteriów wyboru może budzić niezadowolenie części decydentów oraz wpływać negatywnie na wyniki całej instytucji finansowej[155].

Racjonalność działania (w przeciwieństwie do racjonalności decyzji) winna się przejawiać w przedstawianiu kilku możliwych wariantów działania, z których tylko jeden powinien być akceptowalny (jak wiadomo, zaproponowanie rozwiązań nieakceptowalnych jako alternatywnych ułatwia przyjęcie rozwiązania pożądanego). Zgodnie z koncepcją irracjonalności decyzyjnej racjonalny proces decyzyjny może być stosowany jedynie w odniesieniu do spraw drobnych i mało znaczących. Podsumowując założenia tej metody, należy stwierdzić, że w sytuacji decyzji o charakterze strategicznym, gdy konieczne jest podjęcie działania, tradycyjnie rozumianą racjonalność procesu decyzyjnego należy zarzucić[156].

3.1. Propozycje *de lege ferenda*

Rynek finansowy stanowi bez wątpienia jedną z najważniejszych strategicznych sfer życia i aktywności gospodarczej każdego kraju. Państwa zmuszone są podejmować działania zmierzające do zabezpieczenia możliwości bezpiecznego obrotu środkami przez obywateli. Trudność stojąca przed ustawodawcą polega na niełatwym zadaniu uregulowania tej sfery życia w sposób ograniczający możliwość wystąpienia nieprawidłowości, a jednocześnie gwarantujący swobodę obrotu środkami finansowymi. Szczególnie ważnym wyzwaniem stojącym przed ustawodawcą jest opracowanie metod działania oraz określenie źródeł niekorzystnych z punktu widzenia życia gospodarczego zjawisk oraz podjęcie decyzji, w jaki sposób je penalizować i kiedy to robić. Analizy wymagają również procesy prowadzące do podjęcia decyzji ekonomicznych. Taka analiza, przede wszystkim skupiona na regulacjach prawnych, których celem jest zapewnienie uczciwości w działaniu i podejmowaniu decyzji ekonomicznych przez instytucje finansowe, pozwoli

[155] *Ibidem.*
[156] *Ibidem.*

skutecznie przeciwdziałać zjawiskom przestępnym związanym z działalnością na rynku finansowym oraz zabezpieczyć w większym stopniu interes obywateli. Wydaje się, że w polskim systemie prawnym znajduje się szereg regulacji prawnych dotyczących sfery rynku finansowego, którym poświęcona została duża uwaga doktryny. Nie w każdym przypadku, jak się wydaje, ustawodawca sprostał jednak trudnemu zadaniu należytego uregulowania przedmiotowej sfery życia gospodarczego. Dalsze rozważania będą miały na celu zaproponowanie nowych rozwiązań prawnych, w wyższym stopniu zabezpieczających działalność instytucji finansowych oraz proces podejmowania przez nie decyzji gospodarczych, w celu zapewnienia uczciwości oraz zgodności z prawem operacji finansowych podejmowanych na rynku finansowym.

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe
Art. 171.
Kto bez zezwolenia prowadzi działalność polegającą na gromadzeniu środków finansowych, w szczególności pieniędzy, kruszców oraz papierów wartościowych, innych osób fizycznych, osób prawnych lub jednostek organizacyjnych niemających osobowości prawnej, w celu udzielania kredytów, pożyczek pieniężnych lub obciążenia ryzykiem pod jakimkolwiek tytułem zwrotnym, podlega grzywnie do 10 000 000 złotych lub karze pozbawienia wolności do lat 5.
Tej samej karze podlega, kto, prowadząc działalność zarobkową wbrew warunkom określonym w ustawie, używa w nazwie jednostki organizacyjnej niebędącej bankiem lub do określenia jej działalności lub reklamy wyrazów „bank" lub „kasa".
Tej samej karze podlega także ten, kto dopuszcza się czynu określonego w ust. 1 lub 2 działając w imieniu lub w interesie, osoby prawnej lub jednostki organizacyjnej niemającej osobowości prawnej.
Kto, będąc obowiązany do podania uprawnionym organom informacji dotyczących banku i klientów banku w zakresie ustawowego obowiązku, podaje nieprawdziwe lub zataja prawdziwe dane, podlega grzywnie lub karze pozbawienia wolności do lat 3.
Kto, będąc obowiązany do zachowania tajemnicy bankowej, ujawnia lub wykorzystuje informacje stanowiące tajemnicę bankową, niezgodnie

z upoważnieniem określonym w ustawie, podlega grzywnie do 1 000 000 złotych lub karze pozbawienia wolności do lat 3[157].

Z uwagi na znaczenie, jakie ustawodawca przypisuje działalności bankowej oraz z uwagi na towarzyszące temu ryzyko, wprowadzone zostały istotne wymogi, których spełnienie weryfikowane jest przed wydaniem zezwoleń na utworzenie banku oraz podjęcie działalności[158]. Szczegółowość ograniczeń oraz charakter koniecznych do spełnienia wymogów podyktowany jest chęcią ochrony interesów klientów poprzez niedopuszczenie do działalności na rynku podmiotów niespełniających warunków oraz dających rękojmię prawidłowej analizy zagrożeń oraz umiejętności przeciwdziałania im. Sankcje przewidziane przez art. 171 Prawa bankowego gwarantować mają ochronę określeń, takich jak „bank" czy „kasa" przed podmiotami nieuprawnionymi, co ma na celu ochronę klientów oraz zapewnienie im świadomości podejmowania decyzji finansowych. Działanie to stawia jednocześnie w sytuacji uprzywilejowanej podmioty spełniające ustawowe wymogi oraz legalnie prowadzące działalność bankową, gdyż chronione są one przed czynami nieuczciwej konkurencji, takimi jak sprzeczne z prawem działanie zagrażające interesom przedsiębiorców oraz klientów. W szczególności będą więc to przypadki wprowadzającego w błąd oznaczenia przedsiębiorstwa czy nieuczciwa reklama. Działaniem niezgodnym z prawem będzie więc w sytuacji świadczenia usług bankowych bez wymaganych prawem zezwoleń, a także bezprawne reklamowanie się przez dany podmiot jako bank lub kasa, co stanowi sposób na wprowadzenie klientów w błąd. Nazwa przedsiębiorstwa musi być sformułowana w sposób niepowodujący błędnego utożsamiania jej przez klientów z innym podmiotem. Zauważyć należy, że ochrona ta rozciąga się na wszystkie przypadki, gdy sposób sformułowania nazwy może wprowadzać klientów w błąd, nie tylko na w stosunku do podmiotów działających w tej samej branży. Dodatkowo ochrona konsumentów wzmocniona jest regulacjami zastrzegającymi użycie wyrazów takich jak „bank", „bankowy", „kasa" itp. w firmie danego podmiotu, o ile spełnia on wymogi ustawowe do prowadzenia działalności regulowanej jako „bank", „kasa" itp. Niedopuszczalne

[157] Dz.U. 1997 r. Nr 140, poz. 939.
[158] F. Zoll, *Prawo bankowe. Komentarz*, Kraków 2005.

jest umieszczanie tych określeń w firmach podmiotów niespełniających ustawowych warunków. Uzasadnieniem takiego kształtu regulacji jest fakt, że większość społeczeństwa nie posiada specjalistycznej wiedzy, a zastrzeżone wyrazy w bezpośredni sposób sugerują w powszechnym odczuciu, iż ma się do czynienia z instytucją będącą bankiem oraz w związku z tym dającą zgodną z ustawą gwarancję zabezpieczenia interesów potencjalnych klientów. Ważnym kryterium służącym ocenie podobieństwa są więc rodzaj porównywanych usług, a także miejsce ich świadczenia. Regulacja zakazująca wprowadzania w błąd obejmuje swym zakresem normowania całość firmy. Brzmienie całości elementów firmy nie powinno być sprzeczne z zasadą prawdziwości firmy. Niedozwoloną praktyką będzie również naśladownictwo polegające na oferowaniu usług charakterystycznych dla działalności bankowej, takich jak przyjmowanie depozytów na procent itp. Czynem zabronionym będzie prowadzenie działalności bankowej przez podmioty nieuprawnione. Podmioty takie utrudniają w praktyce dotarcie instytucjom działającym zgodnie z prawem do klientów, klientom zaś do podmiotów świadczących poszukiwanie usługi na wysokim i profesjonalnym poziomie.

Oddzielne zagadnienie stanowi sposób uregulowania działalności przestępczej powiązanej z funkcjonowaniem banków oraz świadczeniem usług bankowych. W praktyce dotyczy to przestępczości gospodarczej oraz przestępstw przeciwko mieniu znajdujących się w Kodeksie karnym. Odrębną kwestię stanowią natomiast przestępstwa mające miejsce w sektorze bankowym, popełniane przez podmioty działające jako banki oraz tzw. „parabanki”[159]. Prawo bankowe zawiera tylko jeden przepis odnośnie do przestępstw bankowych, tj. art. 171 Prawo bankowe. Przepis ten, z uwagi na swą budowę, budzi jednak liczne wątpliwości interpretacyjne w praktyce orzeczniczej oraz doktrynie. Z uwagi na ten fakt zasadne wydaje się podjęcie próby jego analizy oraz nowelizacji.

W art. 171 ustawy pr. bank. wskazano siedem kategorii czynów zabronionych oraz określono sankcje karne grożące za ich popełnienie. Przepis ten ma służyć ochronie dóbr takich jak:

– **Stabilność systemu bankowego** wyrażająca się w przeciwdziałaniu występowania przypadków prowadzenia działalności bankowej przez

[159] W. Srokosz, *Instytucje parabankowe w Polsce*, Warszawa 2011.

podmioty nieuprawnione, nieposiadające wymaganych zabezpieczeń personalnych, majątkowych i technicznych. Uważa się, iż podmioty te nie dają rękojmi należytego wykonywania swojej działalności;

– **Bezpieczeństwo systemu bankowego**, którego ochrona realizowana jest przez konstruowanie odpowiednich ram instytucjonalnych działalności bankowej, umożliwiających szybkie i skuteczne przeciwdziałanie zagrożeniom dla tego systemu przez same instytucje bankowe przy pomocy wykwalifikowanych pracowników oraz dzięki odpowiednio sprawowanemu nadzorowi;

– **Zaufanie do systemu bankowego**, istotną cechę omawianego systemu, będącą skutkiem nie tylko rozwiązań instytucjonalnych (np. reglamentowanie działalności bankowej i wymóg wykonywania jej wyłącznie przez podmioty dające rękojmię odpowiedniego poziomu świadczonych usług), jak również postrzegania działalności bankowej jako szczególnego rodzaju działalności, opartej na dyskrecji i przekonaniu, że informacje powierzone instytucjom bankowym podlegają starannej ochronie.

Cechą charakterystyczną przestępstw określonych w art. 171 pr. bank. jest odmienność dóbr prawnych będących przedmiotem ochrony[160]. Kodeks karny nie poświęca wiele uwagi ochronie wymienionych dóbr. Nie ulega wątpliwości, że są one swoiste dla realiów systemu bankowego i to w przepisach poświęconych temu systemowi należy się doszukiwać konkretnych przykładów udzielanej im ochrony. Oczywiście przestępstwa stypizowane w art. 171 pr. bank. objęte są, ze względu na treść art. 116 k.k. oraz brak wyraźnego wyłączenia, regulacjami zawartymi w części ogólnej prawa karnego. Istotną cechą tych przestępstw jest także określenie kar grożących za ich popełnienie najczęściej w drodze koniunkcji. Czyny zabronione określone w art. 171 pr. bank., pomijając ust. 6–8, ze względu na użycie spójnika „i", wskazują na potrzebę kumulatywnego nałożenia kary grzywny oraz wymierzenia kary pozbawienia wolności. Oczywiście, skład orzekający może dążyć do ograniczenia tego efektu poprzez miarkowanie wysokości kary. Niegdyś powodem pewnych kontrowersji była kwestia minimalnej kary, a konkretnie, czy w jej zakresie dopuszczalne jest orzeczenie kary grzywny w wysokości 1 złotego, czy może minimalną orzekaną karą grzywny musi kara w wysokości

[160] P. Ochman, *Ochrona działalności bankowej w prawie karnym. Przepisy karne ustaw bankowych*, Warszawa 2011.

jednokrotności stawki dziennej. Należy zauważyć, że k.k. nie zawiera sztywnego kwotowego podziału stawek[161]. W związku z powyższym niezasadne wydaje się odwoływanie się przy obliczaniu minimalnej wysokości grzywny do stawek dziennych, w sytuacji w której górna granica możliwej do wymierzenia grzywny określona jest w sposób dokładny. Wątpliwości w tej kwestii rozwiewają jednak przepisy wprowadzające Kodeks karny, wskazując, że gdy brak określenia minimalnej wysokości grzywny, będzie ona wynosić sto złotych. Zasadny wydaje się pogląd postulujący zamienienie spójnika „i" na spójnik „lub". Zmiana taka umożliwiłaby sędziom większą swobodę w procesie orzekania. Ponadto tak znowelizowany przepis umożliwiłby wyeliminowanie szkodliwego z punktu widzenia autorytetu i racjonalności prawa zjawiska orzekania grzywien o minimalnej wysokości, wynikającego z obowiązku orzeczenia jednocześnie kary grzywny oraz – jak się wydaje dotkliwszej – kary pozbawienia wolności.

Kształt przepisów penalizujących pierwszy z czynów zabronionych w art. 171 prowadzi do wniosku, że ich celem jest ochrona interesów zarówno klientów, jak i samych banków. Eliminuje to podmioty nieposiadające odpowiednich zezwoleń. Chodzi więc o podmioty, które nie chcą lub nie są w stanie ponosić ciężarów związanych z ochroną interesów klientów, a które mogłyby zdobywać w ten sposób nieuczciwą przewagę nad podmiotami, które wymogi ustawowe spełniają. Art. 171 ust. 1 stanowi, że karana jest działalność podmiotów polegająca na gromadzeniu środków pieniężnych innych podmiotów, w celu świadczenia usług kredytowych, pożyczkowych lub innych rodzajów obciążania tych środków ryzykiem. Czyn ten ścigany jest w trybie publicznoskargowym. Ma ono charakter formalny, z uwagi na fakt, że samo abstrakcyjne ryzyko związane z obciążeniem wkładów ryzykiem stanowi podstawę do odpowiedzialności. Kształt regulacji wskazuje, że jest to również przestępstwo kierunkowe.

Przepis ten w obecnej formie posiada także inne niedoskonałości. Prawdopodobnie z uwagi na przeoczenie przepis ten ignoruje istnienie innych niż pieniężne środków mogących stanowić nośnik wartości ekonomicznej. Wykładnia językowa znamion omawianego czynu zabronionego każe przypuszczać, że nie obejmuje on swoim zakresem niedozwolonego

[161] R.A. Stefański, *Kodeks karny. Komentarz*, Warszawa 2017.

gromadzenia środków, takich jak złoto, obligacje, kryptowaluty itp. Niemożliwe wydaje się, z uwagi na specyfikę prawa karnego oraz związaną z nią potrzebę precyzyjności, aby przepis ten mógł być wykładany w sposób rozszerzający. Dlatego zasadna wydaje się nowelizacja przepisu poprzez zmianę treści w sposób, który umożliwiłby uwzględnienie gromadzenia innych nośników wartości ekonomicznej, takich jak np. kruszce. Wydaje się, że dotychczasowa treść przepisu, mówiąca wyłącznie o środkach pieniężnych, wynika z faktu, iż ustawodawca bezrefleksyjnie powielił treść art. 5 ust. 1 pkt 1 ustawy, mówiącego o wkładach pieniężnych.

W ust. 4 omawianego przepisu stypizowane zostało przestępstwo wprowadzenia uprawnionych do informacji organów w błąd poprzez podanie im nieprawdziwych, bądź też zatajenie prawdziwych, danych dotyczących banku i jego klientów. Przedmiotem znacznych kontrowersji jest, czy omawiany przepis odnosi się wyłącznie do tajemnicy bankowej (pogląd podzielany przez takich przedstawicieli doktryny, jak K. Płończyk czy F. Zoll). Zgodnie natomiast z poglądem przeciwnym, wskazany ustęp odnosi się także do innych danych, nieobjętych ochroną wynikającą z tajemnicy bankowej. Brzmienie przepisu, przedmiot jego ochrony oraz brak odesłań do innych artykułów zdają się wskazywać, że poprawny jest pogląd drugi. W treści ust. 4 brak jest klauzuli zawężającej jego stosowanie jedynie do tajemnicy bankowej, nie odsyła on również do innych przepisów, które takowe ograniczenie by zawierały. W związku z powyższym ust. 4 poddawany jest powszechnej krytyce – jest on wyjątkowo niejasny, co znacząco utrudnia jego stosowanie. W trosce o pewność i skuteczność prawa należałoby zatem rozważyć zmianę jego brzmienia na: „Kto, będąc obowiązany do podania uprawnionym organom informacji dotyczących banku i klientów banku w zakresie ustawowego obowiązku […].

Modyfikacja brzmienia przepisu polegająca na dodaniu frazy „w zakresie ustawowego obowiązku" będzie jasno wskazywać, że chroni on każde żądanie udzielenia informacji, kierowane przez uprawniony organ. Omawiane rozwiązanie zakończy w efekcie trwający stan niepewności co do zakresu ust. 4.

Podkreślenia wymaga również, że ze względu na brzmienie przepisu mamy tu do czynienia z przestępstwem indywidualnym. Na podstawie ust. 4 odpowiedzialność karną można przypisać jedynie osobom, na których ciążył ustawowy obowiązek udzielenia informacji na temat banku i jego klientów. Analizowanego przestępstwa nie może popełnić osoba, która

dobrowolnie podjęła się zachowania tajemnicy bankowej (np. w zawartej umowie). W przypadku naruszenia takiego zobowiązania możliwe będzie przypisanie takiej osobie odpowiedzialności jedynie na podstawie art. 266 § 1 k.k.[162], według którego osoba, która zgodnie z przyjętym na siebie zobowiązaniem, ujawnia lub wykorzystuje informację, z którą zapoznała się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Do zachowania tajemnicy bankowej zobowiązane są wszystkie podmioty posiadające informacje chronione, również te instytucje, które weszły w ich posiadanie w dalszej kolejności dzięki swym uprawnieniom. Regulacja zawarta w art. 171 ust. 5 będzie obejmować różnego rodzaju biegłych, rewidentów, komorników lub sędziów. Niedoskonałością tego przepisu jest jego kategoryczne sformułowanie. Charakterystyczne jest stanowisko przedstawicieli doktryny postulujące nowelizację w celu unormowania możliwości ujawnienia tajemnicy bankowej, w sytuacji, gdy natura stosunku prawnego lub czynności bankowej wymaga takiego kroku lub gdy na takie działanie wyraża zgodę podmiot, którego tajemnica dotyczy. Z uwagi na wagę oraz konsekwencje prawne związane z ujawnieniem tajemnicy bankowej, możliwości takiej nie powinno się domniemywać lub zakładać jej istnienia na podstawie wykładni. Konieczne wydaje się uregulowanie tej kwestii bezpośrednio w ustawie. Za zasadne uznać należy więc dodanie do przepisu stwierdzenia, że:

> Przestępstwa nie popełnia ten, kto ujawnia taką informację, gdy jest to konieczne ze względu na charakter wykonywanej czynności bankowej lub gdy osoba, której informacje są objęte tajemnicą, wyrazi na ujawnienie zgodę.

> Ustawa z dnia 6 czerwca 1997 r. Kodeks karny
> Art. 299. § 1. Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące bezpośrednio lub pośrednio z popełnionego przestępstawa, przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji, pomaga do przenoszenia ich

[162] *Ibidem.*

własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
§ 2. Karze określonej w § 1 podlega, kto będąc pracownikiem lub działając w imieniu lub na rzecz banku, instytucji finansowej lub kredytowej lub innego podmiotu, na którym na podstawie przepisów prawa ciąży obowiązek rejestracji transakcji i osób dokonujących transakcji, przyjmuje, wbrew przepisom, środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, dokonuje ich transferu lub konwersji, lub przyjmuje je w innych okolicznościach wzbudzających uzasadnione podejrzenie, że stanowią one przedmiot czynu określonego w § 1, lub świadczy inne usługi mające ukryć ich przestępne pochodzenie lub usługi w zabezpieczeniu przed zajęciem.
§ 3. (uchylony)
§ 4. (uchylony)
§ 5. Jeżeli sprawca dopuszcza się czynu określonego w § 1 lub 2, działając w porozumieniu z innymi osobami, podlega karze pozbawienia wolności od roku do lat 10.
§ 6. Karze określonej w § 5 podlega sprawca, jeżeli dopuszczając się czynu określonego w § 1 lub 2, osiąga znaczną korzyść majątkową.
§ 6a. Kto czyni przygotowania do przestępstwa określonego w § 1 lub 2, podlega karze pozbawienia wolności do lat 3.
§ 7. W razie skazania za przestępstwo określone w § 1 lub 2, sąd orzeka przepadek przedmiotów pochodzących bezpośrednio albo pośrednio z przestępstwa, a także korzyści z tego przestępstwa lub ich równowartość, chociażby nie stanowiły one własności sprawcy. Przepadku nie orzeka się w całości lub w części, jeżeli przedmiot, korzyść lub jej równowartość podlega zwrotowi pokrzywdzonemu lub innemu podmiotowi.
§ 8. Nie podlega karze za przestępstwo określone w § 1 lub 2, kto dobrowolnie ujawnił wobec organu powołanego do ścigania przestępstw informacje dotyczące osób uczestniczących w popełnieniu przestępstwa oraz okoliczności jego popełnienia, jeżeli zapobiegło to popełnieniu innego przestępstwa; jeżeli

sprawca czynił starania zmierzające do ujawnienia tych informacji i okoliczności, sąd stosuje nadzwyczajne złagodzenie kary[163].

Dotychczasowe brzmienie art. 299 ustawy z dnia 6 czerwca 1997 r. Kodeks karny stanowiło powód wielu sporów w doktrynie. Użyte w nim ogólne stwierdzenia były źródłem wielu niejasności oraz rozbieżności również w praktyce orzeczniczej. Problemy interpretacyjne sprawiał zwłaszcza zwrot „pochodzący z korzyści związanych z popełnieniem czynu zabronionego". Nie brakowało osób twierdzących, że omawiany artykuł dotyczy zarówno zysków pochodzących bezpośrednio, jak i pośrednio z przestępstwa. Zgodnie z innym popularnym poglądem art. 299 obejmował swym zakresem wyłącznie zyski pochodzące pośrednio z czynu zabronionego. Przedstawiciele doktryny (np. W. Wróbel), podzielający pogląd pierwszy, podkreślają, że w omawianym przepisie chodzi również o składniki majątkowe będące bezpośrednim owocem danego przestępstwa (może tu chodzić np. o mienie pochodzące z kradzieży). W przypadku zachowania tożsamości podmiotu, którego mienie stało się przedmiotem przekształceń majątkowych (zastępowanie przedmiotów i praw pochodzących bezpośrednio z przestępstw innymi dobrami), każde mienie uzyskane w wyniku takiego przekształcenia może zostać uznane za przedmiot czynności wykonawczej przestępstwa stypizowanego w art. 299 k.k. Za tzw. brudne pieniądze należy również uznać składniki majątkowe wyszczególnione w § 1 omawianego przepisu, zdobyte w zamian za przedmioty pochodzące bezpośrednio z przestępstwa. Nie ma przeciwwskazań, by do tej kategorii nie zaliczyć także pożytków prawnych z rzeczy takich jak: zapłata za używanie lub odsetki. Przepis w obecnym brzmieniu spotyka się jednak z krytycznymi głosami przedstawicieli doktryny. Na uwagę zasługuje pogląd A. Michalskiej-Warias, która wskazuje że, zgodnie z literalnym brzmieniem przepisu, przedmiotem czynności wykonawczych przestępstwa prania pieniędzy nie mogą być przedmioty uzyskane bezpośrednio z przestępstwa, a jedynie wartości majątkowe uzyskane w zamian za korzyści pochodzące z przestępstwa. Nie ulega wątpliwości, że objęcie zakresem omawianego przepisu jedynie operacji wykonywanych w późniejszych etapach prania pieniędzy, gdy dochodzi do zamiany korzyści pochodzących z przestępstwa

[163] Dz.U. 1997 r. Nr 88, poz. 553.

na inne dobra, byłoby nieracjonalne i nieefektywne. Przekonanie o wadliwym skonstruowaniu regulacji poświęconej przestępstwu prania pieniędzy zdaje się podzielać również J. Bojarski. Podkreśla on, że oparcie się interpretatora na literalnym brzmieniu przepisu prowadzi do wniosku, że analizowany przepis nie obejmuje swoim zakresem środków pochodzących z przestępstwa, lecz uzyskanych w zamian za nie korzyści. Należy jednak zauważyć, że taki wynik interpretacji art. 299 k.k. zostałby osiągnięty z całkowitym pominięciem stosowanej pomocniczo wykładni celowościowej, zgodnie z którą należałoby uznać, że celem przedmiotowej regulacji jest penalizacja zjawiska prania pieniędzy w ogóle, zarówno więc korzyści pochodzących z przestępstwa pośrednio, jak i bezpośrednio. Przyjęcie poglądu przeciwnego prowadziłoby w efekcie do dopuszczenia sytuacji, w której formy prania pieniędzy, uznawane powszechnie przez kryminologów za takowe, nie wypełniałyby znamion przestępstwa wskazanych w ustawie. Do tożsamych wniosków dochodzi także J. Duży, trafnie zauważając, iż wykładnia terminu „pranie brudnych pieniędzy", dla uniknięcia kolizji z normami dotyczącymi czynu paserstwa, wymaga odwołania się przy stosowaniu prawa przede wszystkim do chronionego dobra oraz charakteru czynności wykonawczych tych typów przestępstw[164]. Nie wydaje się kontrowersyjne stwierdzenie, że analiza przepisu pod kątem dobra będącego przedmiotem jego ochrony ma fundamentalne znaczenie dla procesu wykładni i wyznaczenia zakresu przestępstwa. Dokonując wykładni omawianego pojęcia, należy wspomnieć o ratyfikowanej przez Polskę Konwencji Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu. W rozumieniu Konwencji przez pojęcie „dochody" rozumie się korzyść ekonomiczną uzyskaną bezpośrednio lub pośrednio z przestępstw. Przez korzyść ekonomiczną rozumie się tu zarówno korzyści materialne, jak i niematerialne, ruchomości lub nieruchomości, a także dokumenty i inne przedmioty stanowiące dowód posiadania tytułu do mienia lub prawa na mieniu. Przez użyty w Konwencji termin „przestępstwa bazowe" rozumie się przestępstwo, w wyniku którego pozyskano dochody mogące być przedmiotem przestępstwa prania pieniędzy. Przytoczone regulacje wskazują, że podjęte przez Polskę zobowiązania

[164] J. Duży, *Korzyści w przestępstwie prania pieniędzy*, „Prokuratura i Prawo" 2010, nr 12.

o charakterze międzynarodowym przewidują przeciwdziałanie praniu brudnych pieniędzy o pośrednim oraz bezpośrednim skutku[165].

Przedstawiciele doktryny podzielający drugi z poglądów wskazują, że w polskim Kodeksie karnym znane jest już przestępstwo paserstwa. Wskazuje się, że nabywanie korzyści majątkowych pochodzących z przestępstwa wypełnia właśnie znamiona tego czynu zabronionego. Nieuzasadniona wydaje się więc wykładania art. 299 k.k. w sposób rozszerzający obejmująca również zakresem normowania operacje dokonywane na przedmiotach pochodzących bezpośrednio z przestępstwa. Charakterystyczny pogląd występujący w doktrynie, podzielany również przez J. Skorupka, każe sądzić, iż art. 299 k.k. reguluje nieco inne sytuacje, mianowicie nie wymaga się w nim, aby badane środki miały przestępcze pochodzenie. Dobra nie muszą pochodzić z przestępstwa bezpośrednio, muszą natomiast pochodzić z korzyści związanych z przestępstwem. Dla uznania danych środków za „brudne" wystarczające jest wykazanie, że pochodzą one z korzyści związanych z popełnieniem czynu zabronionego. Przedmiotowa regulacja nie ogranicza się więc do sytuacji, gdy dane dobro pochodzi bezpośrednio z przestępstwa[166]. Uznać należy więc, że art. 291 k.k. oraz art. 299 k.k. dotyczą dwóch odmiennych sytuacji. Należy odróżnić pojęcia takie jak „przedmiot uzyskany za pomocą czynu zabronionego" oraz „przedmiot pochodzący z korzyści związanych z związanych z popełnieniem czynu zabronionego". Wydaje się, że pogląd skupia się na założeniu, że oba przepisy regulują odmienne sytuacje. W przypadku art. 299 k.k. chodzi o sytuację, gdy dobro, którym się rozporządza, pochodzi z zysków odniesionych z przestępstwa. Zauważalny jest trend w orzecznictwie każący pod pojęciem „dóbr uzyskanych za pomocą czynu zabronionego" rozumieć rzeczy, które uzyskało się poprzez dokonanie czynu zabronionego. Niedopuszczalne wydaje się więc mylenie przedmiotu pochodzącego z przestępstwa z przedmiotem pochodzącym z korzyści uzyskanych w związku z popełnieniem przestępstwa. Rozważania te prowadzą do wniosku, że przedmioty pochodzące bezpośrednio z czynu zabronionego nie będą mogły być uznane za spełniające wymogi ustawowe oraz uzasadniające

[165] *Idem*, *Zorganizowana przestępczość podatkowa w Polsce. Zwalczanie przestępczego nadużycia mechanizmów podatkowych VAT i akcyzowego*, Warszawa 2013.

[166] J. Skorupka, *Pojęcie „brudnych pieniędzy" w prawie karnym*, „Prokuratura i Prawo" 2006, nr 11.

zastosowanie art. 299 k.k. Omawiane wątpliwości są dostrzegane również przez orzecznictwo[167]. Istnieje linia orzecznicza wskazująca, że przestępstwo prania pieniędzy dotyczyć może wyłącznie przedmiotów uzyskanych za pomocą przestępstwa. Pozostawia to jednak otwartym kwestie tego, co należy uczynić w sytuacji, gdy ów łańcuch majątkowy jest dłuższy i chodzi o dobra jedynie pośrednio pochodzące z przestępstwa. Odpowiedzią na ten problem wydaje się właśnie rozwiązanie przewidziane w art. 299 k.k., który dotyczy właśnie wartości innych niż osiągnięte bezpośrednio, co odróżniać ma przestępstwo prania pieniędzy od paserstwa. Regulacja zawarta w art. 299 znajduje więc zastosowanie w innej, szerszej kategorii czynów. W zamyśle ustawodawcy konieczne jest więc zanalizowanie, czy sprawca czynu zabronionego wszedłby w posiadanie określonych dóbr również w sytuacji, gdyby nie popełniono wcześniej pierwotnego przestępstwa. Korzyść, co wielokrotnie potwierdzało orzecznictwo, rozumieć przy tym należy szeroko, może nią być zarówno uzyskanie nowych środków lub spłata części zobowiązań. W związku z powyższymi rozważaniami wydaje się, że istnieje potrzeba nowelizacji art. 299 poprzez uwzględnienie zarówno charakteru bezpośredniego, jak i pośredniego dóbr, których dotyczy. Celowa wydaje się zamiana treści przepisu, tak, aby jej literalne brzmienie odpowiadało przyjętym liniom orzeczniczym oraz aby wykładnia celowościowa dokonywana przez sądy mogła znaleźć potwierdzenie również w wykładni językowej regulacji. Nie budzi wątpliwości fakt, że zbyt ogólnikowe sformułowanie omawianego przepisu prowadzi do problemów praktycznych, które muszą być rozwiązywane przez orzeczenia Sądu Najwyższego. Należy jednak wskazać, że niedopuszczalna jest sytuacja, w której o odpowiedzialności karnej decyduje celowościowa wykładnia sądu, co do zasady niezgodna z wykładnią językową. Wydaje się, że w takiej sytuacji konieczna jest legislacyjna interwencja ustawodawcy w celu rozwiązania problemu.

[167] Sygn. akt II AKz 417/09.

3.2. Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych

Źródłem licznych sporów i kontrowersji jest również uregulowana w Kodeksie spółek handlowych kwestia nieważności uchwały zgromadzenia spółki kapitałowej[168]. Bez względu na podejście, jakie przyjmiemy w stosunku do uchwały zgromadzenia, czy będziemy ją traktować jako czynność prawną, czy jako inne zdarzenia prawne, nieważność uchwały zgromadzenia, stwierdzanie zaistnienia faktu nieważności oraz jej skutki są jednym z specyficznych zagadnień prawa handlowego, odbiegającym od rozwiązań prawa cywilnego[169]. Różnica pomiędzy skutkami nieważności czynności prawnej przyjętymi w Kodeksie cywilnym a skutkami nieważności uchwały wydaje się mieć oparcie w konflikcie wartości prawa handlowego, z których jedne przemawiają za wyeliminowaniem wadliwej uchwały z obrotu, podczas gdy inne uzasadniają utrzymanie uchwały w obrocie prawnym. Zdarza się zatem, iż uchwała, co do której istnieje podstawa do stwierdzenia nieważności, zachowuje moc obowiązywania. Należy podkreślić, że choć podniesienie zarzutu nieważności uchwały jest możliwe w każdej sytuacji, to samo ustalenie nieważności uchwały w drodze odpowiedniego powództwa wymaga już spełnienia wymagań dotyczących terminów oraz zakresu podmiotowego takiego wniosku. Wspomniane ograniczenia nie są jedynymi stosowanymi przez ustawodawcę w celu zachowania mocy obowiązującej przez niektóre wadliwe uchwały. Nieraz zdarza się, że katalog przesłanek nieważności czynności prawnej w stosunku do uchwały wadliwej zgromadzenia ulega zawężeniu.

Wydaje się, że ideą przyświecającą rodzimemu ustawodawcy jest, aby każda sytuacja sprzeczności uchwały zgromadzenia z prawem mogła potencjalnie stanowić podstawę jej nieważności. Stwierdzenia nieważności należy dochodzić w drodze powództwa sądowego lub poprzez podniesienie zarzutu nieważności w trakcie toczącego się postępowania. Zgodnie z literalnym brzmieniem art. 252 § 1 oraz art. 425 § 1 KSH dostateczną podstawą do zastosowania sankcji nieważności uchwały jest każde naruszenie prawa związane z procesem jej podejmowania. Sąd Najwyższy zdaje się łagodzić niezwykle surową wykładnię omawianych przepisów, ograniczając możliwość

[168] Dz.U. 2000 r. Nr 94, poz. 1037.
[169] R. Uliasz, *Nieważność uchwały zgromadzenia spółki kapitałowe*, Warszawa 2018.

stwierdzenia nieważności uchwały do wypadków, w których podczas podejmowania uchwały miało miejsce uchybienie formalne mogące wpływać na jej treść. W świetle przeprowadzonych rozważań należy stwierdzić, że pozostawianie przepisów dotyczących nieważności uchwały w ich obecnym brzmieniu jest błędem. Analiza rozwiązań problemu nieważności uchwał w innych porządkach prawnych prowadzi do przekonania, iż rozwiązanie krajowe jest w istocie niechlubnym wyjątkiem na mapie instytucji prawnych krajów europejskiej tradycji prawnej.

3.3. Niemcy

Ustawodawca niemiecki wyróżnia dwa typy wadliwości uchwał walnego zgromadzenia:

- wzruszalność,
- wadliwość.

W związku z powyższym wyróżnia się uchwały, które mogą być podważone przy wykorzystaniu powództwa o uchylenie uchwały (*Anfechtungsklage*), oraz uchwał o stwierdzenie nieważności uchwały *(Nichtigkeitsklage*). Wzruszalność uchwały walnego zgromadzenia została uregulowana przede wszystkim w § 243–248a AktG, zaś nieważność m.in. w § 241–242 i 249 AktG. W pewnym uproszczeniu można powiedzieć, że powództwo o uchylenie uchwały (*Anfechtungsklage*) stanowi odpowiednik znanego w prawie polskim powództwa z art. 249 § 1 i art. 422 § 1 KSH, zaś powództwo o stwierdzenie nieważności (*Nichtigkeitsklage*) odpowiada powództwu z art. 252 i 425 KSH. Należy jednak zaznaczyć, że ekwiwalentność pomiędzy tymi instrumentami prawnymi można przyjmować jedynie z pewną ostrożnością, bowiem podstawy do wniesienia obu powództwa na gruncie obu porządków nie są tożsame.

Należy zauważyć, że o nieważności uchwały można w niemieckim porządku prawnym mówić w zasadzie jedynie wtedy, gdy doszło do enumeratywnie wymienionych w ustawie naruszeń, mających postać sprzeczności uchwały z prawem, przy czym chodzi tu zarówno o sprzeczności o charakterze formalnym, jak i sprzeczność z prawem o charakterze materialnym[170]. Natura

[170] *Ibidem.*

sankcji nieważności uchwały wyraża się w tym, że w razie spełnienia się określonych w ustawie przesłanek nieważności wadliwa uchwała od początku nie wywołuje zamierzonych skutków prawnych, przy czym sankcja występuje z mocy prawa, a zatem niezależnie od tego, czy określona osoba podjęła kroki zmierzające do wykazania tej postaci wadliwości. Z uwagi na fakt, że nieważność istnieje *ex lege*, oznacza, że przesłanki uzasadniające nieważność uchwały są uwzględniane z urzędu przez sąd rejestrowy. Prawo niemieckie przewiduje następujące przesłanki nieważności uchwały:

- Brak zwołania walnego zgromadzenia,
- Brak zaprotokołowania uchwały,
- Niezgodności uchwały z naturą spółki,
- Naruszenie przepisów mających na celu wyłączenie lub przede wszystkim ochronę wierzycieli spółki lub inny sposób mających chronić interes publiczny,
- Naruszenie dobrych obyczajów,
- Uchylenie uchwały jako nieważnej w oparciu o przepisy ustawy o postępowaniu w sprawach rodzinnych i postępowaniu nieprocesowym.

Wzruszalność uchwały oznacza stan, w którym uchwała dotknięta określonymi wadami proceduralnymi lub odnoszącymi się do treści danej uchwały może być wyeliminowana z obrotu w oparciu o prawomocny wyrok o charakterze kształtującym[171]. W przeciwieństwie jednak do techniki legislacyjnej zastosowanej przy określaniu przesłanek nieważności uchwały wyliczenie przesłanek uzasadniających zastosowanie sankcji wzruszalności nie ma jednak charakteru wyczerpującego. Przyjęta przez niemieckiego ustawodawcę konstrukcja przepisów dotyczących wzruszalności uchwały polega na tym, że sformułowano w zasadzie dwie ogólne przesłanki warunkujące uchylenie uchwały (§ 143 ust. 1 i 2 AktG), a następnie wskazano wprost, które postacie wadliwości nie mogą prowadzić do skutku w postaci unicestwienia uchwały, nawet wtedy, gdyby rzeczywiście zostały spełnione (§ 243 ust. 3 i 4 AktG). Zgodnie z literalnym brzmieniem § 243 ust. 1 AktG wzruszenie uchwały uzasadnia każde naruszenie statutu lub ustawy, niemniej orzecznictwo i doktryna są zgodne co do tego, że wspomniany przepis należy interpretować restrykcyjnie. Wyjaśnienie tego podejścia wymaga uprzedniego odniesienia się do

[171] U. Huffer, C. Schaffer, *Münchener Kommenta*, München 2010.

dwóch konkurujących ze sobą teorii, tj. teorii przyczynowości oraz teorii istotności. Zgodnie z pierwszą z nich, wzruszalność uchwały może opierać się na naruszeniu ustawy lub statutu, jednak na skarżącym nie ciąży obowiązek wykazania, że dane naruszenie mogło mieć wpływ na treść uchwały. To pozwana spółka, jeżeli chce doprowadzić do oddalenia powództwa, musi dowieść, że podnoszone przez powoda naruszenie pozostawało bez wpływu na treść uchwały. Teoria przyczynowości dominowała w starszym orzecznictwie. Natomiast począwszy od końca 2001 r. w judykaturze sądu federalnego zaczęto w szerszym zakresie uwzględniać teorię istotności. W tym ujęciu jako kluczowe przy ocenie, czy dana uchwała kwalifikuje się do uchylenia, czy też powinna zostać zachowana w obrocie, zwłaszcza w razie naruszenia obowiązków informacyjnych, powinno zostać uwzględnione to, czy „obiektywnie oceniający akcjonariusz", mając wiedzę w danej sprawie, oddałby głos innej treści niż w rzeczywistości. Zaskarżenie uchwały stawało się więc uzasadnione wtedy, gdy przed akcjonariuszami zatajono informacje istotne dla kierunku głosowania akcjonariuszy. Teoria istotności została ostatecznie przyjęta przez ustawodawcę na gruncie § 243 ust. 4 zd. 1 AktG. Niemiecka ustawa przewiduje następujące przesłanki wzruszalności uchwały:

- Sprzeczność uchwały z ustawą lub statutem,
- Uzyskanie przez akcjonariusza lub inne osoby szczególnych korzyści ze szkodą dla spółki lub innych akcjonariuszy.

Wyraźna wydaje się tendencja na gruncie niemieckiego prawa spółek zmierzająca do ograniczenia podstaw do stwierdzenia nieważności uchwał, w stosunku do przesłanek uzasadniających nieważność czynności prawnych na gruncie „ogólnego" prawa cywilnego. Doktryna wydaje się podzielona w ocenie przedmiotowego zjawiska. Pojawiają się głosy mówiące, że surowe enumeratywne określenie zamkniętego katalogu przesłanek stanowi zbyt wielkie ustępstwo na rzecz zachowania wadliwej uchwały w obrocie, kosztem pominięcia pewnych, czasami istotnych uchybień.

3.4. Szwajcaria

Podobnie jak ma to miejsce w innych systemach prawnych, również w prawie szwajcarskim wyróżnia się w zasadzie dwie sankcje wadliwości uchwał walnego zgromadzenia, a mianowicie wzruszalność, która została uregulowana w art. 706–706a OR, oraz nieważność, którą uregulowano w art. 706b OR.

Istota sankcji nieważności polega na tym, że uchwała dotknięta tą postacią wadliwości od samego początku nie wywołuje skutków prawnych, tj. od chwili jej podjęcia[172]. Z tego względu nieważność jest uwzględniana z urzędu, zarówno przez sądy, jak i organy administracji, w tym organ prowadzący rejestr handlowy (*Handelsregisterfuhrer*)[173].

Wyraźne brzmienie art. 706b OR, gdzie ustawodawca posługuje się terminem „w szczególności" pozwala przyjąć, że wyliczenie przesłanek nieważności uchwały walnego zgromadzenia ma charakter jedynie przykładowy, zaś katalog tych przesłanek ma charakter otwarty. Taki też jest kierunek wykładni art. 706b OR prezentowany w doktrynie i w orzecznictwie. Zauważyć należy, że zasadniczo zgodnie ze szwajcarskim prawem nie może do nieważności uchwały prowadzić sprzeczność jej treści ze statutem. Odmiennie sytuacja prezentuje się jedynie w sytuacji, gdy normy statutowe kształtują tryb zwołania zgromadzenia lub tryb podjęcia uchwały. W takim przypadku możliwe jest przyjęcie nieważności uchwały. Do przesłanek uzasadniających uznanie uchwały za nieważną należą w szczególności:

- Wyłączenie lub ograniczenie niektórych praw akcjonariuszy,
- Ograniczenie akcjonariuszom prawa kontroli w większym stopniu niż na to zezwala ustawa,
- Naruszenie podstawowych struktur spółki akcyjnej lub przepisów o ochronie kapitału.
- Inne przesłanki, nieokreślone enumeratywnie.

Natura sankcji wadliwości postrzegana jest w prawie szwajcarskim podobnie do tego jak to ma miejsce w prawie niemieckim. Uchwała z chwilą ogłoszenia wywołuje skutki prawne, niemniej byt uchwały od momentu upływu terminu do jej zaskarżenia znajduje się w zawieszeniu. W tym okresie należy

[172] D. Dubs, R. Truffer, *Basler Kommentar*, Basel 2018.
[173] R. Uliasz, *op. cit.*

liczyć się z tym, że uchwała może zostać zaskarżona. Skutki prawne i definitywna ważność uchwały podlegają zatem warunkowi rozwiązującemu, którym jest skuteczność zaskarżenia. Wzruszalność bywa definiowana jako nieważność warunkowa lub zawieszona, ponieważ byt prawny uchwały zależy od skuteczności potencjalnego powództwa. Jeżeli powództwo o uchylenie uchwały zostanie uwzględnione, to wystąpi w istocie skutek w postaci nieważności uchwały. Uwzględnienie powództwa oznacza bowiem uchylenie uchwały ze skutkiem *ex tunc*. Taki sposób pojmowania wzruszalności ma istotne znaczenie z punktu widzenia wykonalności chwały. Uchwała wzruszalna, nawet jeżeli zostanie zaskarżona, jest bowiem wykonalna, możliwe jest co najwyżej żądanie tymczasowego odroczenia w czasie skutków przez nią wywołanych. Do przesłanek pozwalających na uchylenie uchwały prawo szwajcarskie zalicza:

- Ograniczenie lub pozbawienie akcjonariuszy praw, z naruszeniem ustawy lub postanowień statutu,
- Bezpodstawne pozbawienie akcjonariuszy przysługujących im uprawnień lub ich ograniczenie,
- Nieuzasadnione celami spółki nierówne traktowanie lub dyskryminację akcjonariuszy,
- Zniesienie celu zarobkowego spółki bez zgody wszystkich akcjonariuszy.

Warto zauważyć, że również szwajcarska doktryna posługuje się pojęciem „uchwał nieistniejących". Podobnie jak w prawie polskim jest to pojęcie pozanormatywne. Chodzi tu o takie stany faktyczne, których nie można przyjąć, że uchwała doszła do skutku, gdyż albo nie odbyło się, w sensie prawnym, walne zgromadzenie, albo uchwały nie podjęto, bo nie zostały spełnione istotne wymogi związane z jej podjęciem[174]. Doktryna szwajcarska opisuje więc oprócz uchwał nieważnych także uchwały pozorne i nieistniejące. Kryteria podziału między tymi pojęciami nie są jednak zwykle jasne.

Wydaje się, że spośród jurysprudencji szwajcarskiej dominuje zapatrywanie zakładające konieczność zachowania w obrocie wadliwych uchwał, również tych naruszających porządek prawny, jeżeli wymagałaby tego zasada pewności obrotu.

[174] D. Dubs, R. Truffer, *op. cit.*

3.5. Włochy

Ustawodawca włoski wskazuje na dwa rodzaje sankcji wadliwych uchwał podejmowanych na zgromadzeniu spółki kapitałowe:

- wzruszalność uchwał (art. 2377–2378 wł. k.c.),
- nieważność uchwał (art. 2379–2379 ter wł. k.c.)

Dualizm sankcji wadliwych uchwał zgromadzeń spółek kapitałowych opiera się na dualizmie sankcji wadliwych czynności prawnych. Na gruncie prawa włoskiego można zatem mówić o czynnościach wzruszalnych, które mogą zostać wyeliminowane z obrotu prawnego za pomocą powództwa o uchyleniu skutków prawnych danej czynności prawnej[175], a także o czynnościach prawnych dotkniętych nieważnością, których eliminacji służy powództwo o stwierdzeniu nieważności[176]. Czynność prawna wzruszalna od samego początku wywołuje skutki prawne, jednak mogą one zostać niejako unicestwione w razie uwzględnienia odpowiedniego powództwa. Skutki mają więc charakter czasowy i nietrwały. Wady uzasadniające wzruszenie nie mogą być jednak rozpatrywane z urzędu. Według art. 2377 wł. k.c. uchwały zgromadzenia, podjęte zgodnie z wymogami prawa oraz postanowieniami statutu, są wiążące dla wszystkich wspólników. Uchwały, które nie zostały podjęte zgodnie z prawem bądź postanowieniami statutu, mogą zostać zaskarżone przez podmioty wymienione w tym przepisie. Sankcja wzruszalności uchwały zgromadzenia opiera się więc na dwóch przesłankach, z których każda samodzielnie uzasadnia uchylenie wadliwej uchwały. Charakterystycznie wadliwość wynikająca z naruszenia ustaw i wadliwość wynikająca z naruszenia norm pozaprawnych, tj. norm statutowych, traktowane są równorzędnie.

Istota nieważności uchwały w prawie włoskim polega na uznaniu, że przedmiotowa uchwała od samego początku nie wywołuje skutków prawnych. Sądy zobowiązane są do uwzględniania nieważności z urzędu. Charakterystyczną cechą włoskiej nieważności jest jej „nieuzdrawialność", tzn. uchwała dotknięta taką sankcją nie może podlegać konwalidacji, a odpowiednie powództwa, kontestujące nieważną czynność, nie są ograniczone terminem. Po gruntownej reformie włoskiego prawa spółek z 2004 r. nieważność uchwał zgromadzenia

[175] *Manuale di istituzioni di diritto privato*, a cura di M. di Pirro, Neapol 2018.
[176] F. Rocchio, A. Liserre, *Lezioni di diritto privato*, 2017.

spółek kapitałowych została uregulowana w art. 2379, art. 2379 bis oraz art. 2379 ter wł. k.c. Reforma dokonała istotnej modyfikacji dotychczasowego katalogu przesłanek stwierdzenia nieważności uchwał. W obecnym stanie prawnym włoski kodeks wskazuje następujące przesłanki nieważności uchwał:

- Brak zwołania zgromadzenia,
- Brak protokołu,
- Niemożliwość lub sprzeczność z prawem celu uchwały.

Należy zauważyć, że przesłanki nieważności uchwał zgromadzenia spółki kapitałowej obejmują o wiele węższy zakres stanów faktycznych niż przesłanki uchylenia uchwały. Z uwagi na sposób regulacji uzasadniona wydaje się teza, że włoski Kodeks cywilny w zakresie zaskarżania uchwał opiera się na zasadzie maksymalnej stabilności uchwał podejmowanych przez zgromadzenia, jak również nawiązanych na ich podstawie stosunków[177].

3.6. Wnioski dla prawa polskiego

Na tle prowadzonych rozważań porównawczoprawnych zauważyć należy, że nie do pogodzenia z wartościami, jakimi jest m.in. potrzeba zachowania bezpieczeństwa obrotu i trwałości stosunków wewnątrzkorporacyjnych oraz relacji spółki z osobami trzecimi, wydaje się regulacja prawna, w świetle której każda postać sprzeczności uchwały z ustawą może prowadzić do stwierdzenia nieważności uchwały w drodze wyroku sądowego w ramach relatywnie długich terminów ustawowych bądź do bezterminowego podniesienia zarzutu nieważności uchwały. Należy zauważyć, że w przypadku jednakowego traktowania przez ustawodawcę poważnych uchybień, jak i tych mniej znaczących sprawia, że w przypadku najpoważniejszych postaci wadliwości nie ma możliwości ich kwestionowania w drodze powództwa sądowego po upływie terminów zawitych. Może zdarzyć się tak, że uchwała zgromadzenia zobowiązuje zarząd np. do zachowań przestępczych lub też zmienia przedmiot działalności spółki w ten sposób, że przewiduje działalność z bezwzględnie obowiązującymi przepisami prawa. Wydaje się, że w takim przypadku ranga uchybień przemawia za dopuszczalnością kwestionowania wadliwej uchwały po upływie terminów

[177] M. Sferrazza, *Appunti di diritto commerciale*, 2011.

zawitych. Podobnie może mieć miejsce sytuacja, gdy tryb podjęcia uchwały jest dotknięty poważnymi uchybieniami proceduralnymi, które miały wpływ na treść uchwały. Wyłączenie możliwości kwestionowania ważności uchwały po upływie terminów zawitych stanowi, jak się wydaje, zbyt duże ustępstwo w kierunku zasady trwałości stosunków wewnątrzkoropracyjnych lub relacji nawiązanych przez spółkę z osobami trzecimi, umniejsza natomiast w stopniu nieuzasadnionym zasadę praworządności[178]. Rozwiązanie, zgodnie z którym rażące formy wadliwości uchwały mogą być podniesione również w późniejszym czasie wyłącznie jako zarzut, nie wydaje się rozwiązywać problemu w stopniu wystarczającym. Takie rozwiązanie prowadzi bowiem do sytuacji, w których nawet gdy uchwała dotknięta jest poważnymi wadami wynikającymi z naruszenia prawa, o ile nie zostanie podniesiony zarzut, sąd zmuszony jest do przejścia nad tym do porządku dziennego. Wydaje się, że najbardziej rażące formy uchybień, czy to względem norm materialnoprawnych, czy to norm proceduralnych, powinny być uwzględniane z urzędu. Celowe wydaje się w tym miejscu rozważenie nowelizacji i przyjęcia rozwiązania podobnego do znanego w systemie włoskim. Kompetencja tak, a powinna przysługiwać zarówno sądom rejestrowym, jak i sądom w postępowaniach spornych. Ponadto należy zauważyć, że niezależnie od wagi uchybienia, krąg osób i organów uprawnionych do zaskarżenia uchwały powództwem o stwierdzenie nieważności jest identyczny[179]. Zasadność takiego rozwiązania może budzić wątpliwości. Można postawić tezę, że przynajmniej w niektórych przypadkach legitymacja czynna do zaskarżenia uchwały powinna być określona szerzej, niż to ma miejsce w obecnie obowiązujących przepisach. Celowe wydaje się poszerzenie kręgu uprawnionych o zastawników akcji lub udziałów, a także o odwołanych członków organów, bo umożliwiłoby tym osobom zaskarżenie uchwał zgromadzenia dotkniętych szczególnie rażącymi uchybieniami. Należy również zauważyć, że istniejące rozwiązania zakładające nieważność uchwały zgromadzenia opierają się na sprzeczności uchwały z prawem, zaś wzruszalność jest konsekwencją naruszenia norm pozaprawnych (umownych, statutowych), prowadzą do paradoksu. Może bowiem dojść do naruszenia ustawowego wymogu tajności głosowania, w ten sposób, że przeprowadzono głosowanie

[178] Z. Jara, *Kodeks spółek handlowych. Komentarz*, Warszawa 2017.
[179] A. Kidyba, *Kodeks spółek handlowych. Komentarz*, Warszawa 2017.

jawne, w sytuacji, gdy jeden z uczestników głosowania zażądał głosowania w trybie tajnym. Nie powinno budzić wątpliwości, że w takim przypadku istnieje podstawa do stwierdzenia nieważności uchwały. Jednocześnie może dojść do sytuacji, w której umowa spółki z o.o. ustanawia wymóg głosowania tajnego w sprawach nieobjętych hipotezą art. 247 § 2 zd. 2 KSH (tajność głosowania zostaje rozciągnięta na stany faktyczne nieobjęte treścią tego przepisu). W tym przypadku wymóg tajności głosowania w oznaczonych sprawach odzwierciedla wolę wszystkich osób zawierających umowę spółki, jednak naruszenie tego wymogu mogłoby prowadzić co najwyżej do uchylenia uchwały, a nie do jej nieważności, bowiem nie mamy tu do czynienia z naruszeniem ustawy, ale normy o charakterze pozaprawnym. W konsekwencji tam, gdzie źródłem obowiązku przeprowadzenia głosowania w trybie tajnym jest wola jednego uczestnika (zgłaszającego odpowiednie żądanie w trybie art. 247 § 2 zd. 2 KSH), mielibyśmy do czynienia z uchwałą nieważną. Wydaje się, że odpowiedzią na pojawiające się problemy mogłoby być co do zasady zrównanie sankcji za naruszenie ustawy i statutu spółki. Nie w znaczeniu wcielenia w życie koncepcji, która legła u podstaw sposobu zaskarżania wadliwych uchwał zgromadzeń w KH z 1934 r., ale o takie sformułowanie przepisów, które – pozwalając na kontestowanie uchwał sprzecznych z ustawą i umową spółki, co do zasady, jednym i tym samym powództwem – umożliwiałoby jednocześnie w znacznie szerszym zakresie, niż to ma miejsce obecnie, powoływanie się na szczególnie ciężkie postaci uchybień normom prawnym. Ta rozszerzona dopuszczalność podnoszenia wyjątkowo poważnych postaci naruszeń popełnionych w trakcie podejmowania uchwały lub szczególnie istotnych uchybień normom materialnoprawnym znajdowałaby wyraz zarówno w braku ograniczeń czasowych, jak i podmiotowych względem powództwa zmierzającego do ustalenia, że do takiego istotnego naruszenia porządku prawnego doszło. Rozwiązanie takie pozwoliłoby wyeliminować pojawiającą się jeszcze w polskim piśmiennictwie konstrukcję uchwał nieistniejących, która to wyrasta z przekonania doktryny, że sankcja nieważności z art. 252 § 1 i art. 425 § 1 KSH w niektórych przypadkach jest niewystarczająca. Do podobnego procesu odchodzenia od koncepcji uchwał nieistniejących doszło w drodze nowelizacji we Włoszech i Hiszpanii. Wydaje się, że jedynie najsurowsze formy naruszenia przepisów powinny stanowić podstawę do stwierdzenia nieważności uchwały. Uchwała powinna być uznana za nieważną, gdy w sposób jaskrawy narusza normy

prawa, godząc tym samym w obowiązujący porządek prawny, gdy jednocześnie ranga naruszanych norm jest znaczna. Byłyby to stany faktyczne, jak np. wybór przez zgromadzenie na członka władz spółki osoby skazanej za przestępstwa określone w art. 18 § 2 KSH. Zasadne byłoby opracowanie przez ustawodawcę enumeratywnie przesłanek nieważności uchwały, podobnie jak ma to miejsce w ustawodawstwie niemieckim lub włoskim. Uelastycznieniu modelu mogłoby służyć wykorzystanie konstrukcji klauzul generalnych, jak np. znana z systemu hiszpańskiego klauzula porządku publicznego. Odnośnie do naruszeń norm proceduralnych zasadne byłoby uwzględnić w ustawodawstwie przywoływaną wcześniej zasadę istotności, tak aby tylko takie naruszenia miały wpływ na unicestwienie uchwały.

3.7. Ustawa z dnia 27 lipca 2002 r. Prawo dewizowe

Art. 11.

1. Działalność kantorowa jest działalnością regulowaną w rozumieniu przepisów ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców i wymaga wpisu do rejestru działalności kantorowej, zwanego dalej „rejestrem".
2. Przepisów o działalności kantorowej nie stosuje się do banków, oddziałów banków zagranicznych oraz do instytucji kredytowych i oddziałów instytucji kredytowych[180].
3. Przepisy o działalności kantorowej stosuje się do podmiotów zajmujących się działalnością polegającą na wymianie walut wirtualnych i walut konwencjonalnych.

Z uwagi na charakter prowadzonej działalności wydaje się zasadne objęcie działalności polegającej na pośrednictwie oraz organizowaniu punktów wymiany walut wirtualnych na walutę konwencjonalną przepisami prawa dewizowego odnoszącymi się do działalności kantorowej. Działalność ta zasadniczo polega na tym samym, jedyną różnicą jest fakt, że waluta wirtualna nie jest walutą gwarantowaną przez żadne państwo. Wydaje się, że w celu ochrony osób dokonujących transakcji na rynku kryptowalut, a także w celu

[180] Dz.U. 2002 r. Nr 141, poz. 1178.

zapewnienia pełnej transparentności oraz przeciwdziałania zjawiskom przestępczym związanym z unikaniem opodatkowania oraz praniem brudnych pieniędzy konieczna jest interwencja ustawodawcy. Z uwagi na charakter technologiczny oraz konstrukcję zdecentralizowaną, opartą na poszczególnych użytkownikach danego systemu kryptowalut, jedynym racjonalnym wyjściem zmierzającym do kontroli nad przedmiotowym zjawiskiem oraz przeciwdziałania przestępczości wydaje się działanie skupione na instytucjach wymiany oraz „bankowych" rynku walut wirtualnych. Pozwali na uchwycenie i regulację podstawowej infrastruktury koniecznej dla działanie tego zjawiska, mianowicie podmiotów umożliwiających przechowywanie środków oraz ich wymianę na waluty konwencjonalne.

Z uwagi na ten fakt zasadne wydaje się znowelizowanie ustawy poprzez dodanie do art. 11 ustawy paragrafu trzeciego o treści:

> § 3. Przepisy o działalności kantorowej stosuje się do podmiotów zajmujących działalnością polegającą na wymianie walut wirtualnych i walut konwencjonalnych.

Regulacja tak będzie się wiązała z koniecznością uzyskania przez podmioty chcące prowadzić przedmiotową działalność zezwolenia od uprawnionego organu. Aby takie zezwolenie uzyskać, podmiot ów będzie musiał spełnić szereg wymogów, w tym wymogów informacyjnych. Pozwoli to na kontrolę zjawiska handlu walutami wirtualnymi oraz przeciwdziałanie przestępczości z tym związanej.

3.8. Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym[181]

Przedmiotowa ustawa reguluje organizację, zakres i cel sprawowania nadzoru nad rynkiem finansowym, w którego skład wchodzi nadzór bankowy, nadzór emerytalny, nadzór ubezpieczeniowy, nadzór nad rynkiem kapitałowym, nadzór nad instytucjami płatniczymi oraz m.in. nadzór uzupełniający. Ustawa reguluje również powstanie oraz funkcjonowanie Komisji

[181] Dz.U. 2006 r. Nr 157, poz. 1119.

Nadzoru Finansowego. Z uwagi na głośne skandale związane z korupcją oraz zjawisko tzw. obrotowych drzwi z urzędów państwowych do biznesu wydaje się zasadne opracowanie rozwiązań mających przeciwdziałać ewentualnym nadużyciom oraz konfliktom interesów. Rozwiązaniem problemów związanych z tym zjawiskiem wydaje się wdrożenie regulacji wprowadzającej roczną karencję uniemożliwiającą zatrudnienie byłych pracowników urzędu zajmujących stanowiska szczebla dyrektorskiego oraz członków komisji w podmiotach podlegających nadzorowi Komisji Nadzoru finansowego. Zasadna wydaje się nowelizacja ustawy o nadzorze nad rynkiem finansowym przez dodanie artykułu 10a o treści:

> Art. 10a
> 1. Członkowie Komisji Nadzoru Finansowego oraz kierownicy departamentów, dyrektorzy i ich zastępcy, nie mogą podejmować przez okres 12 miesięcy od dnia wypowiedzenia bądź rezygnacji z pracy w Komisji, pracy w podmiotach podlegających nadzorowi Komisji Nadzoru Finansowego.
> 2. W wypadku niezachowania terminu 12 miesięcy osoba łamiąca zakaz podlega karze grzywny oraz zakazowi zatrudnienia w administracji publicznej przez okres 10 lat.

ROZDZIAŁ CZWARTY

Analiza zarządzania operacjami w instytucjach finansowych

4.1. Wprowadzenie

Nie ulega wątpliwości, że dla operacji wykonywanych przez instytucje finansowe, rozwoju tych instytucji oraz osiąganie przez nie zysku znaczenie fundamentalne ma efektywność rynku finansowego oraz dostęp jego uczestników do informacji istotnych z ekonomicznego punktu widzenia. W związku z powyższym przeprowadzenie omówienia procesu zarządzania operacjami przez wspomniane podmioty powinno być poprzedzone analizą wskazanych pojęć.

Należy zauważyć, że obecnie mamy do czynienia z rozkwitem usług związanych z zarządem aktywami finansowymi, co ma, jak się wydaje, związek z zamianą aktywów finansowych na instrumenty finansowe. Procesy te mają z kolei wpływ w szczególności na rozwój podmiotów inwestujących w papiery wartościowe.

Z istnieniem rynku finansowego wiążą się czynniki takie jak: rozwój systemu bankowego oraz usług oferowanych przez banki, obniżenie wymagań związanych z przepływem kapitału i dewiz, dynamiczny rozwój handlu, rozwój firm międzynarodowych, globalizacja obrotu gospodarczego[182]. Na podstawie powyższych rozważań uprawnione jest twierdzenie, że odpowiednia ochrona winna być zapewniona rynkowi kapitałowemu, w szczególności zaś podmiotom, których działalność ma związek z instrumentami finansowymi.

Istotność rynku kapitałowego wynika również z tego, że to właśnie debiut spółki na giełdzie wiąże się ze znacznym napływem kapitału, rozwojem konkurencyjności oraz świadczy o prestiżu i dobrej kondycji finansowej. Obecność

[182] A. Samborski, *Rynki papierów wartościowych w krajach Unii Europejskiej*, Katowice 2004.

na giełdzie umożliwia podmiotowi gospodarczemu pozyskanie kapitału oraz realizację projektów wiążących się ze znacznymi kosztami. Należy również podkreślić, że podejmowanie decyzji inwestycyjnych jest procesem wymagającym umiejętności oraz, co najważniejsze, dostępu do rzetelnych informacji[183]. Operacje na rynku giełdowym są dokonywane na podstawie uzyskanych informacji, w związku z czym zapewnienie warunków uczciwej konkurencji wymaga zarówno dostępu do prawdziwych informacji, jak i ochrony prawa do tajemnicy przedsiębiorstwa.

Należy podkreślić, że informacje na rynku finansowym, w szczególności zaś kapitałowym, mają wartość ekonomiczną. Chodzi tu głównie o dane, do których nie ma dostępu większość uczestników rynku – wejście w posiadanie takich informacji daje dużą przewagę nad konkurencją i pozwala osiągać zyski jej kosztem[184]. Informacja na rynkach finansowych ma specyficzny charakter. Z jednej strony jest dobrem chronionym prawem, z drugiej strony natomiast jest warunkiem *sine qua non* istnienia rynku finansowego. Ze względu na wskazaną dwoistą naturę poprawne uregulowanie kwestii informacji na rynku finansowym jest niezwykle problematyczne[185].

Zgodnie z poglądem wyrażanym w doktrynie cena rynkowa stanowi podstawowy nośnik informacji zawierający wszystkie okoliczności istotne dla uczestników rynku[186]. Pojęciem podstawowym dla rynku jest natomiast jego efektywność, w tym także efektywność informacyjna. Przez efektywność należy tu rozumieć racjonalne ekonomicznie gospodarowanie. Polega ono na maksymalizacji efektów i minimalizacji nakładów[187]. Efektywność danego rynku jest jedną z głównych przesłanek, w oparciu o które inwestorzy decydują się na podjęcie ryzyka, co wprost przekłada się na rozwój rynku. Dostęp do informacji ma natomiast podstawowe znaczenie dla tego, czy dany rynek będzie się cieszył popularnością wśród inwestorów. Efektywność ma również istotne znaczenie z punktu widzenia emitentów oraz inwestorów, którzy

---

183 N. Siemieniuk, J. Kilon, *Technologie informatyczne na rynku kapitałowym*, Białystok 2006.

184 M. Górecki, *Informacje poufne na rynku kapitałowym – obowiązki, procedury, sankcje*, „HUK" 2008, nr 1.

185 *Idem*, *Informacje poufne na rynku kapitałowym – podstawowe problemy regulacji prawnej oraz pojęcie informacji poufnej i insidera*, „HUK" 2007, nr 1.

186 *Ibidem*.

187 S. Buczek, *Efektywność informacyjna rynków akcji. Teoria a rzeczywistość*, Warszawa 2005.

postrzegają ją jako wynikową kapitalizacji, płynności, stopy zwrotu współmiernej do ryzyka, bezpieczeństwa obrotu, poziomu kosztów transakcyjnych oraz kosztów pozyskania kapitału[188]. Oprócz omówionej już efektywności możliwe jest jeszcze wyróżnienie wskaźników, takich jak płynność, elastyczność i przejrzystość. Celem zwiększenia możliwości stałego podnoszenia efektywności rynku przy zachowaniu jego bezpieczeństwa i przejrzystości w 2005 r. wprowadzono nowe przepisy regulujące rynek finansowy. Na uwagę zasługuje opinia Komitetu Europejskich Regulatorów Rynku Papierów Wartościowych (CESR), zgodnie z którą istotność danej informacji należy badać, biorąc pod uwagę płynność obrotu danym instrumentem finansowym, średnie wahania jego kursów w okresie poprzedzającym publikację danej informacji, a także stabilność i stopień rozwoju danego rynku[189].

Pojęcie „rynku efektywnego" ma bliski związek z teorią racjonalnych oczekiwań, tłumaczącą zachowanie uczestników rynku w wypadku pojawienia się nowych informacji. Zgodnie z omawianą teorią wszystkie pojawiające się informacje, które są istotne z punktu widzenia sporządzanych prognoz cen instrumentów, mają bezpośredni wpływ na ceny bieżące. Wynika z tego, że zmiana w kształtowaniu się zmiennej powoduje zmianę oczekiwań dotyczących tej zmiennej i jej kształtowania się w przyszłości[190].

Zgodnie z badaniami Komitetu ds. Obligacji, Operacji i Regulacji w Przemyśle w Hongkongu w 1988 r. przestępstwa giełdowe mają znaczący wpływ na efektywność rynku finansowego. Efektywność ta zależy od czynników takich jak: stabilizacja rynku, sprawność jego funkcjonowania, brak manipulacji i oszustw oraz ochrona inwestorów[191].

Efektywność rynku finansowego, w szczególności kapitałowego, przejawia się w trzech sferach: alokacyjnej, operacji (transakcyjna) i informacyjnej[192]. Efektywność alokacyjna jest cechą rynków o wysokiej kapitalizacji

---

188 R. Tuzimek, M. Bańkowski, *Giełda papierów wartościowych w Warszawie – szanse i zagrożenia dalszego rozwoju*, [w:] *Rynki kapitałowe*, red. W. Bień, Warszawa 2005.

189 K. Oplustil, P.M. Wiórek, *Europejskie i polskie regulacje dotyczące informacji poufnych na rynku kapitałowym (cz. I)*, „Prawo Spółek" 2005, nr 2.

190 U. Ziarko-Siwek, *Ocena efektywności informacyjnej wybranych segmentów rynku finansowego w Polsce*, Warszawa 2004.

191 R. Kuciński, *Przestępstwa giełdowe*, Warszawa 2000.

192 W. Sharpe, *Asset Allocation. Management Style and Performance Measurement*, „Journal of Portfolio Management", Winter 1992.

i płynności i wyraża się w możliwości pozyskiwania przez podmioty kapitału do realizacji najlepszych projektów inwestycyjnych[193]. Przez efektywność transakcyjną rozumie się wysoki poziom konkurencji, prawne regulacje, procedury związane z obrotem papierami wartościowymi oraz innowacyjność określane mianem infrastruktury prawnej oraz tzw. infrastruktury instytucjonalnej. Wpływ na nią ma zdolność ustawodawcy do dostosowania przepisów prawa do zmieniających się warunków zarówno obrotu giełdowego, jak i jego zdolność do dostosowania rosnących potrzeb ochrony prawnej uczestników tego obrotu[194]. Efektywność ta definiowana jest również jako mechanizm rynkowy umożliwiający niezwłoczne zawieranie transakcji przy niskim poziomie kosztów[195].

Należy zauważyć, że najważniejszym rodzajem efektywności z punktu widzenia uczestników rynku jest efektywność informacyjna. Wynika to z roli, jaką pełni informacja w procesie inwestycyjnym. Przez stan efektywności informacyjnej rozumie się taki stan, w którym na danym rynku występuje pełny i szybki transfer informacji do wszystkich jego uczestników. Rynek efektywny informacyjnie to taki, w którym dostępne dane o instrumentach finansowych są natychmiast i w całości odzwierciedlone w ich cenach[196]. Cechą rynku efektywnego jest również to, że nowe informacje szybko docierają do wszystkich uczestników rynku, a ceny aktywów finansowych niezwłocznie dostosowują się do nowych informacji[197].

Wspólnymi elementami większości definicji efektywności są: powszechna dostępność do informacji dla wszystkich uczestników rynku, brak kosztów transakcji oraz zgodność uczestników rynku co do wpływu treści nowej informacji na ceny walorów[198]. Cechą rynku efektywnego jest także odzwierciedlanie przez ceny wszelkich dostępnych informacji[199]. Zgodnie z niektórymi głosami w doktrynie na rynku efektywnym informacyjnie nie powinny

---

193 *Ibidem*.

194 P. Kulpaka, *Giełdy w gospodarce*, Warszawa 2007.

195 U. Ziarko-Siwek, *op. cit.*

196 P. Kulpaka, *op. cit.*

197 J. Czekaj, M. Woś, J. Żarnowski, *Efektywność giełdowego rynku akcji w Polsce. Z perspektywy dziesięciolecia*, Warszawa 2001.

198 H. Gurgul, *Analiza zdarzeń na rynkach akcji. Wpływ informacji na ceny papierów wartościowych*, Kraków 2006.

199 S. Buczek, *op. cit.*

występować koszty transakcyjne, a informacje powinny być powszechnie dostępne oraz oceniane przez uczestników rynku pod kątem bieżących i przyszłych cen akcji[200]. Dalej należy zauważyć, że w każdym momencie ceny poszczególnych aktywów uwzględniają informacje z przeszłości oraz informacje dotyczące oczekiwanych w przyszłości zdarzeń[201]. Większość rynków charakteryzuje się jedynie średnim poziomem efektywności informacyjnej. Zakłada on kierowanie się przez uczestników rynku zarówno informacjami zawartymi w sprawozdaniach finansowych spółek, jak i: w cenach, raportach bieżących i okresowych, a także innych dostępnych analizach i raportach branżowych. Mając na uwadze powyższe rozważania, możliwe staje się wymienienie informacji mających wpływ na wartość instrumentów finansowych. Będą to przede wszystkim podane do publicznej wiadomości informacje o emitencie, informacje o historycznych cenach walorów oraz prywatne informacje o emitencie[202].

Według innego prezentowanego w doktrynie poglądu rynek jest efektywny informacyjnie, jeśli ceny aktywów pozostają bez zmian po ujawnieniu informacji wszystkim uczestnikom rynku[203].

W ramach idealnie efektywnego informacyjnie rynku finansowego badaniu podlegają wszystkie informacje mogące wpłynąć na wysokość cen, zarówno te jawne, jak i te niejawne. Ważne jest również, by uczestnicy obrotu giełdowego mieli równy dostęp do informacji. Oczywistym jest jednak, że poszczególni uczestnicy rynku w różnym czasie uzyskują dostęp do poszczególnych informacji, co w praktyce uniemożliwia istnienie pełnej efektywności informacyjnej. Należy podkreślić, że wymuszenie pełnej efektywności informacyjnej byłoby sprzeczne z samą ideą gry rynkowej.

Należy również wskazać odmienną, konkurencyjną do teorii efektywnego rynku teorię anomalii. Teoria ta zakłada szereg odstępstw od pełnego i niezwłocznego odzwierciedlenia wartości informacji w cenie instrumentu finansowego.

Możliwe jest także wyróżnienie w ramach omawianej teorii tzw. anomalii: czasowych, które wynikają ze spóźnionej reakcji inwestorów na pojawiające się

---

200 *Ibidem*.
201 U. Ziarko-Siwek, *op. cit.*
202 H. Gurgul, *op. cit.*
203 *Ibidem*.

informacje. Oprócz tego wskazać należy tzw. nadreakcje rynku na efekt przegrania – zwycięzcy oraz anomalie związane z charakterystyką spółek. Charakterystyczne dla polskiego rynku są zakłócenia wywoływane przez uczestników rynku prowadzących tzw. grę marketingową oraz wspomniane już opóźnione reakcje inwestorów[204].

Podsumowując, informacja ma podstawowe znaczenie dla rynków finansowych. Wpływa zarówno na proces podejmowania decyzji inwestycyjnych, jak i na atrakcyjność i efektywność rynku, będąc wszakże objęta ochroną. Przedmiotem ochrony są tak informacje poufne i informacje stanowiące tajemnicę zawodową, jak sama informacja oraz prawo do uzyskania informacji.

4.2. Modele zarządzania w instytucji finansowej

Jak już wspomniano, dla osiągnięcia sukcesu na rynku finansowym konieczne jest długoterminowe planowanie. Zarządy powinny formułować strategie, czyli koncepcje jego systemowego funkcjonowania nastawione na osiąganie zysków i ograniczanie ryzyka. Realizacja strategii instytucji finansowej wymaga natomiast zastosowania odpowiednich narzędzi, w tym metod zarządzania, które umożliwią urzeczywistnienie założeń zawartych w strategii. Celem niniejszego fragmentu opracowania jest zaproponowanie i omówienie konkretnych sposobów zarządzania operacjami instytucji finansowych.

4.3. *Reengineering*

Reengineering, inaczej techniczna reorganizacja procesów działania, zakłada stopniową poprawę działalności podmiotu przez techniczną reorganizację istotnych z punktu widzenia prowadzonej działalności procesów, maksymalizację wartości dodanej powstającej w toku tych procesów oraz minimalizację wszelkich zbędnych elementów[205].

[204] S. Buczek, *op. cit.*
[205] M. Capiga, J. Harasim, G. Szustak, *Finanse banków*, Warszawa 2005.

Decydując się na *reengineering*, nie wolno zapominać o konieczności zidentyfikowania zarówno celów strategicznych, jak i tych tworzących wartość dodaną. Należy również pamiętać, że usprawnieniu powinny podlegać zarówno same procesy najważniejsze, jak i wszystkie powiązane z nimi procedury, elementy struktury organizacyjnej (dobrym przykładem może tu być zlecenie analizy czynności instytucji finansowej podmiotom zewnętrznym)[206].

Podstawą zastosowania omawianej metody zarządzania jest uprzednie dogłębne zrozumienie uwarunkowań rynku, na którym się działa, oraz specyfiki klientów, co ma umożliwić ciągłe dostosowywanie do nich konkretnych procedur.

Aby ukazać sposób stosowania omawianej metody w bieżącej działalności instytucji finansowej, należy posłużyć się przykładem.

Jednym ze sposobów, w jaki omawiane podmioty mogą uzyskać przewagę nad konkurencją na rynku finansowym, jest usprawnianie procesu świadczenia usług. Usprawnienie wspomnianego procesu winno przebiegać tak, by dostosować świadczoną usługę do potrzeb potencjalnego klienta, takich jak np. krótki okres oczekiwania na pozytywną decyzję w przypadku wniosków kredytowych. Osoba odpowiedzialna za sformułowanie planu reformy wewnętrznej winna dokonać analizy problemów występujących na czterech płaszczyznach[207]:

- problemy związane z kadrą,
- problemy związane z rozwiązaniami technologicznymi,
- problemy związane z procesami,
- problemy związane z klientami.

W odniesieniu do pierwszej sfery, jeżeli chodzi o wspomniane już wnioski kredytowe, istotnym problemem, który wpływa na wydłużenie procedury kredytowej, jest nieefektywny podział zadań wśród pracowników, co przekłada się na rozmycie odpowiedzialności oraz spowolnienie procesu decyzyjnego. Usprawnienie mogłoby zatem polegać na ograniczeniu liczby pracowników obsługujących konkretną sprawę – pozwoliłoby to na szybsze wydawanie decyzji oraz określenie osób za nie odpowiedzialnych.

---

[206] R.L. Manganelli, M.M. Klein, *Reengineering. Metoda usprawnienia negocjacji*, Warszawa 1998.

[207] J. Peppard, R. Rowland, *Reengineering*, Warszawa 1997.

W przypadku rozwiązań technologicznych należy wskazać na potrzebę wykorzystania oprogramowania i sprzętu przygotowanego z myślą o konkretnej działalności świadczonej przez daną instytucję. Pewna automatyzacja oraz ograniczenie czynnika ludzkiego niewątpliwie wpłynie na szybkość procesu oraz jego bezpieczeństwo.

W odniesieniu do procesów dobrym pomysłem wydaje się podział czynności dokonywanych przez pracowników instytucji na dwie grupy: pierwszą polegającą na kontakcie z klientem oraz drugą polegającą na niego przez tzw. zaplecze. Usprawnienie w podanym przykładzie powinno polegać na wykształceniu jednej jednostki w strukturze organizacyjnej instytucji, odpowiedzialnej za obsługę kierowanych do niej wniosków. Skoncentrowanie w jednym miejscu dokumentacji oraz odpowiedzialności związanej z dokonywanymi operacjami przekłada się na wzrost przejrzystości, bezpieczeństwa oraz szybkości działania instytucji. Dobrym rozwiązaniem jest również opracowanie nowego, centralnego systemu oceny wiarygodności potencjalnego klienta[208].

W odniesieniu do samych klientów należy rozważyć lepsze przygotowanie personelu do kontaktów z nimi. Kontakty z klientem winny charakteryzować się profesjonalizmem, szybkością działania oraz transparentnością.

Jak wykazano, *reengineerig* należy zatem rozumieć jako radykalną zmianę dążącą do zapewnienia satysfakcji klienta oraz efektywności funkcjonowania instytucji. Szczegółowe propozycje usprawnień należy w każdym wypadku formułować dopiero po zapoznaniu się ze specyfiką danego rynku oraz potrzebami klientów instytucji.

4.4. Zarządzanie przez jakość

Głównym założeniem zarządzania przez jakość jest zwiększanie zadowolenia klienta, o które winny zabiegać wszystkie jednostki organizacyjne instytucji, co ma się przekładać na większą efektywność ponoszonych nakładów.

[208] M. Capiga, *Reengineering kredytów detalicznych w polskiej praktyce bankowej*, „Bank i Kredyt" 2001, nr 8.

Przyjmując ten typ zarządzania, należy mieć na względzie, że podstawą zapewnienia wysokiej jakości usług, tzn. pełnej zgodności świadczonego produktu z wymaganiami klienta, jest świadomość oczekiwań klientów. Jakość usług nie powinna sprowadzać się tylko do spełniania wymagań klientów instytucji, lecz powinna je przekraczać i wiązać się ze świadczeniem różnorodnych usług dodatkowych[209].

Należy również zauważyć, że choć głównym celem podmiotów działających na rynku finansowym jest osiąganie zysku, to nie może się to odbywać kosztem jakości usług – taka praktyka w dłuższym okresie czasu prowadzi do pogorszenia sytuacji finansowej podmiotu.

W doktrynie wyróżnić można trzy podstawowe techniki zarządzania przez jakość w sektorze usług finansowych: metodę kompleksowego zarządzania jakością (TQM) oraz metodę audytu jakości (ISO 9000).

Kompleksowe zarządzanie jakością zakłada zaangażowanie całego personelu we wzrost jakości świadczonej usługi. Wszyscy pracownicy instytucji powinni brać udział w programach szkoleniowych, mających na celu zrozumienie odpowiedzialności, wizji i narzędzi związanych z podnoszeniem jakości usług. System ten oparty jest na zorientowaniu zasobów ludzkich instytucji na nieustanne doskonalenie usług po najniższych kosztach i wiąże się z tworzeniem takich wewnętrznych jednostek, jak np. zespoły jakości odpowiedzialne za wyznaczanie standardów i procedur usprawniających działanie instytucji na każdym szczeblu organizacyjnym. Omawiana metoda charakteryzuje się całościowym podejściem oraz zaangażowaniem wszystkich pracowników w poprawę jakości, jednakże wymaga znacznych nakładów finansowych, a jej wprowadzenie trwa dłuższy czas[210].

Drugi z zaproponowanych sposobów zarządzania zakłada dostosowanie świadczonych usług do międzynarodowych standardów jakości zgodnych z British Standards BS 5750. Audyt jakości powinien w szczególności skupiać się na dostosowaniu procedury postępowania z zapytaniami i zażaleniami klientów – chodzi tu nie tylko o szybkie załatwienie sprawy, lecz także o rozpoznanie i zażegnanie problemów. Powyższa metoda wiąże się

[209] J.J. Dahlgaard, K. Kristensen, G.K. Kanji, *Podstawy zarządzania jakością*, Warszawa 2000.

[210] T. Ansell, *Zarządzanie jakością w sektorze usług finansowych. Narzędzia zarządzania jakością oraz ich zastosowanie*, Warszawa 1997.

z przeprowadzaniem audytów zewnętrznych oraz opracowywaniem na ich podstawie procedur mających podnosić jakość usług – stanowi dobrą podstawę do podejmowania dalszych działań. Jej wadą jest znaczna czasochłonność oraz biurokracja, dodatkowo należy też wskazać brak nakierowania na czynnik ludzki – przedmiotem analizy są procedury. Warto zauważyć, że zdobywanie certyfikatów jakości jest najpopularniejszym obecnie systemem tworzenia jakości.

4.5. *Lean management* – strategia „odchudzania"

Istotą omawianej metody jest relokacja zasobów i skoncentrowanie na segmentach rynku i klientach oferujących największy wzrost. Z założenia chodzi zatem o reorganizację struktury organizacyjnej przy jednoczesnym zwiększeniu korzyści klienta w drodze poprawy jakości obsługi i działania. Analizowana koncepcja zakłada przeniesienie poza strukturę organizacyjną instytucji pobocznych rodzajów działalności (tzw. *outsourcing*) oraz zwiększenie integracji obsługi klienta. Równie istotna jest optymalizacja systemu ekonomicznego, która dokonuje się dzięki redukcji złożoności produktu i łączeniu czynności podobnych – standaryzacja procesów ma usprawnić funkcjonowanie i zmniejszyć koszty operacji.

Lean management dąży również do zorientowania organizacji na rynek, co przejawia się w dostosowaniu struktury organizacyjnej do potrzeb klientów (np. specjalne komórki odpowiedzialne za współpracę z VIP-ami czy w dostosowywanie sieci placówek do potrzeb potencjalnych klientów).

Omawiana metoda zarządzania działalnością instytucji finansowej zakłada zatem uproszczenie struktury organizacyjnej, przeniesienie na podmioty zewnętrzne ciężaru usług niezwiązanych z główną działalnością prowadzoną przez instytucję oraz dostosowanie struktury wewnętrznej organizacji do potrzeb i położenia klientów.

4.6. Zarządzanie przez wartość

Omawiana metoda sprowadza się do połączenia zasad i mechanizmów ekonomicznych tworzących wartość z procesami i systemami zarządzania nieodzownymi do wprowadzania ich w życie[211]. Zarządzanie przez wartość można zdefiniować jako działania nakierowane na podwyższenie aktywów firmy, zwiększenie efektywności zużycia zasobów, osiągnięcie wysokiej pozycji rynkowej oraz przewagi konkurencyjnej.

Możliwe jest wyróżnienie dwóch niewyłączających się technik zarządzania przez wartość – *shareholder value* oraz *stakeholders value*[212].

Model pierwszy dąży do maksymalizacji wartości majątku akcjonariuszy. W związku z procesem globalizacji coraz większa uwaga jest przywiązywana przez akcjonariuszy do długoterminowego tworzenie wartości, dlatego też podobna strategia instytucji finansowej sprzyja przyciąganiu inwestorów. Koncepcja kładzie nacisk na zapewnienie trwałości i stabilności wzrostu majątku akcjonariuszy. To właśnie stałość i pewność wzrostu jest w tym wypadku istotnym czynnikiem przekładającym się na wartość majątku akcjonariuszy, a niższe krótkoterminowe zyski mają być równoważone przez stały, choć rozłożony w czasie wzrost.

Model drugi bierze pod uwagę nie tylko interesy akcjonariuszy, ale również innych podmiotów mających interes w wysokiej wartości instytucji. Będą to grupy w jakiś sposób związane z instytucją, uzależnione od jej funkcjonowania, mogące w ograniczonym zakresie wpływać na jej działania[213]. Będą to zarówno klienci, jak i przedstawiciele władz lokalnych, a także środowiska lokalne. Wszystkie te grupy mają bowiem swój udział w kreowaniu wartości instytucji. Instytucja finansowa powinna dołożyć wszelkich starań, by wpływać na grupy powiązane w sposób, który ułatwi jej niezakłóconą pracę oraz przyczyni się do maksymalizacji zysków. Wypracowana w efekcie pozycja instytucji na danym rynku, zaufanie do niej oraz przekonanie o jakości świadczonych przez nią usług, żywione nie tylko przez klientów, ale także przez podmioty mające wpływ na jej działalność, przekładają się na wartość instytucji.

---

[211] J. Świderski, *Zarządzanie bankiem przez wartość*, „Bank i Kredyt" 1999, nr 1–2.
[212] M. Capiga, *Zarządzanie bankiem*, Warszawa 2010.
[213] A. Koźmiński, W. Piotrowski, *Zarządzanie. Teoria i praktyka*, Warszawa 1996.

Podsumowując, należy zaznaczyć, że zaproponowane metody zarządzania operacjami instytucji finansowych nie tylko nie są sprzeczne, lecz wręcz powinny być stosowane łącznie, w zależności od potrzeb danej instytucji. Wybór konkretnej metody lub metod zarządzania powinien uwzględniać czynniki takie, jak zasoby instytucji, możliwości wdrożenia oraz praktyczną potrzebę.

4.7. Postulaty *de lege ferenda*

4.7.1. Wprowadzenie jednolitej licencji bankowej

Punktem wyjścia do omówienia koncepcji jednolitej licencji bankowej powinna być analiza prawa europejskiego w zakresie działalności inwestycyjnej instytucji bankowych. Aktem, w którym zawarto ogólne ramy systemu udzielania licencji na prowadzenie działalności inwestycyjnej, jest dyrektywa MIFID II oraz dyrektywa 2013/36/UE[214]. Zgodnie z motywem 38 w związku z art. 1 ust. 3 dyrektywy MIFID II instytucja kredytowa **nie musi posiadać odrębnego zezwolenia** w celu świadczenia usług inwestycyjnych lub prowadzenia działalności inwestycyjnej. Zatem regulacje europejskie w odniesieniu do banków dotyczą kwestii zezwoleń na świadczenie usług inwestycyjnych, nie zawierają również nakazu wydzielenia stosownej jednostki w strukturze banku[215]. Należy podkreślić, że na mocy omawianej dyrektywy każdy podmiot uprawniony z tytułu licencji oraz kontrolowany przez państwo członkowskie ma prawo do świadczenia usług inwestycyjnych, prowadzenia działalności inwestycyjnej oraz innych dodatkowych objętych zezwoleniem. Ponadto członkowie wspólnoty zobowiązali się nie nakładać na te podmioty żadnych wyjątkowych wymagań o charakterze dyskryminacyjnym. Implementując dyrektywy unijne, polski ustawodawca ma prawo wprowadzać bardziej restrykcyjne rozwiązania, o ile tylko nie różnicuje

[214] Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczania instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz. Urz. UE L 176 z 27.06.2013 r., s. 338–436).

[215] M. Kurzajewski, *Usługi maklerskie*, Warszawa 2014.

podmiotów nimi objętych ze względu na kraj pochodzenia. W efekcie jest możliwe, że instytucje krajowe będą postawione w gorszej sytuacji od instytucji kredytowych działających na terytorium RP w formie oddziału lub działalności transgranicznej. Omawiany mechanizm może być przez to źródłem ograniczeń dla rodzimych instytucji inwestycyjnych[216].

Aby dostosować polskie regulacje dotyczące rynku kapitałowego do m.in. dyrektywy MIFID II oraz rozporządzenia MIFIR[217], w kwietniu 2018 r. weszła w życie ustawa o zmianie ustawy o obrocie instrumentami finansowymi oraz niektórych innych ustaw[218]. Nowe regulacje europejskie koncentrują się na zmianach w zakresie ochrony inwestorów, struktury i przejrzystości rynku instrumentów finansowych. Kwestia udzielania licencji na prowadzenie działalności inwestycyjnej instytucjom bankowymi nie została w nich uwzględniona, przez co w dalszym ciągu trwa stan pewnego dualizmu licencyjnego.

Rozważając możliwe zmiany i usprawnienia systemu wydawania licencji, wydaje się zasadne znowelizowanie ustawy o obrocie instrumentami finansowymi i prawa bankowego w ten sposób, że uchylone zostaną przepisy: art. 70 ust. 2, art. 111–114 oraz art. 119–123 u.o.i.f. Rozwiązaniem najracjonalniejszym byłoby zawarcie całej procedury licencyjnej w prawie bankowym w ramach postępowania w sprawie wniosku o wydanie zezwolenia na utworzenie banku albo w postępowaniu o wydanie zezwolenia na zmianę statutu dla banku już istniejącego[219]. Przyjęcie takiego rozwiązania wymagałoby zmiany art. 6 ust. 1 pr. bank. tak, by bank mógł świadczyć usługi inwestycyjne oraz prowadzić działalność inwestycyjną na zasadach określonych w ustawie o obrocie instrumentami finansowymi. Znowelizowany powinien także zostać art. 69 u.o.i.f. Wydaje się zasadnym odejście w ustawie od pojęć działalności maklerskiej oraz czynności maklerskich. Poświęcone im fragmenty ustawy należałoby zastąpić implementacją sekcji A i B dyrektywy

---

[216] *Ibidem*.

[217] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (EU) nr 648/2012 (Dz. Urz. UE L 173 z 12.06.2014 r.); dalej: „MIFIR".

[218] Ustawa z dnia 1 marca 2018 r. o zmianie ustawy o obrocie instrumentami finansowymi oraz niektórych innych ustaw (Dz.U. poz. 685).

[219] T. Zinkiewicz, *Działalność inwestycyjna banków w świetle jednolitej licencji bankowej*, „Monitor Prawa Bankowego" 2016, nr 3.

MIFID II, czyli wprowadzenie terminów działalności inwestycyjnej oraz usług inwestycyjnych. Dokonanie powyższej zmiany we wszystkich ustawach oraz aktach wykonawczych poświęconych rynkowi finansowemu stanowiłoby dostosowanie prawa polskiego do regulacji europejskich.

Umożliwienie bankom wykonywania działalności inwestycyjnej w drodze jednolitej licencji wymagałoby wprowadzenia ograniczenia w postaci obowiązku powiadamiania Komisji Nadzoru Finansowego o przekroczeniu w ramach działalności inwestycyjnej banku na rachunek własny określonych ustawowo progów. W takim wypadku KNF byłaby upoważniona do zastosowania wobec banku środków, takich jak nakazanie zredukowania aktywności poniżej progów (np. poprzez zbycie aktywów), kary pieniężne oraz zobowiązanie od przekazania działalności inwestycyjnej prowadzonej na rachunek własny banku do podmiotu zależnego. Omawiane zabezpieczenia miałyby na celu zabezpieczenie klientów instytucji przed skutkami lekkomyślnych inwestycji dokonywanych przy użyciu zdeponowanych przez nich środków.

4.7.2. Nieuprawniona działalność bankowa – uzupełnienie luk

Zgodnie z art. 171 ust. 1 ustawy pr. bank., karze podlega osoba, która bez zezwolenia prowadzi działalność polegającą na gromadzeniu środków pieniężnych innych osób fizycznych, prawnych lub jednostek organizacyjnych niemających osobowości prawnej, w celu udzielenia kredytów, pożyczek pieniężnych lub obciążeniem ryzykiem tych środków w inny sposób. Jest to więc występek publicznoskargowy, formalny z uwagi na to, iż obciążenie wkładów ryzykiem jest jedynie abstrakcyjnym zagrożeniem dobra prawnego, natomiast z racji na sformułowanie „w celu" jest przestępstwem kierunkowym, toteż popełnione może być jedynie z zamiarem bezpośrednim[220].

Ustawodawca niepotrzebnie wspomina jedynie o gromadzeniu środków pieniężnych. Z uwagi na wymóg literalnego dekodowania znamion czynu zabronionego oraz istnienie zasady *nullum crimen sine certa* wydaje się, iż poza zakresem penalizacji znajdą się przypadki niedozwolonego gromadzenia

[220] F. Zoll, *Prawo bankowe*, t. 2: *Polsko-Niemieckie Centrum Prawa Bankowego UJ*, Kraków 2005.

środków innych niż pieniężne, takich jak: złoto, obligacje, akcje czy inne papiery wartościowe. Choć część autorów wskazuje na możliwość rozszerzenia wykładni tego przepisu, wydaje się ono nieuzasadnione z uwagi na wymóg precyzyjności określania przepisów prawa karnego. Poza zakresem sporu pozostają waluty obce, które z całą pewnością należy uznać za środki pieniężne[221].

Należy również zwrócić uwagę na nieuregulowanie przez ustawodawcę sytuacji, w której podmiot posiadający stosowne zezwolenie wykonuje działalność bankową, czyni to jednak wbrew warunkom określonym w jego treści. Zachowanie nie jest zawarte w chwili obecnej wprost w hipotezie omawianego przepisu, co może prowadzić do poważnych wątpliwości co do przestępnego charakteru wykraczania poza ograniczenia określone w zezwoleniu.

W związku z powyższym zasadna wydaje się zmiana brzmienia art. 171 ust. 1 poprzez zamianę określenia „środków pieniężnych" na „składników majątku" oraz zamiana zwrotu „kto bez zezwolenia" na „kto bez zezwolenia lub wbrew jego treści". Zmieniony ust. 1 brzmiałby wówczas:

> Art. 171. 1. Kto bez zezwolenia **lub wbrew jego treści** prowadzi działalność polegającą na gromadzeniu **składników majątku** innych osób fizycznych, osób prawnych lub jednostek organizacyjnych niemających osobowości prawnej, w celu udzielania kredytów, pożyczek pieniężnych lub obciążania ryzykiem tych środków w inny sposób, podlega grzywnie do 10 000 000 złotych i karze pozbawienia wolności do lat 5.

Powyższa zmiana pozwoliłaby zakończyć stan niepewności wywołany nieadekwatnym, niekompletnym określeniem zawartym obecnie w ustawie.

---

[221] A. Mazur, B. Pyka, M. Utracka, *Przestępstwa określone w prawie bankowym. Analiza art. 171 ustawy prawo bankowe. Problemy wykładnicze regulacji w świetle realiów obrotu bankowego*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 37.

4.7.3. Waluty wirtualne – prawne środki płatnicze

W dniu 29 marca 2018 r. prezydent RP podpisał ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu. W akcie tym dokonywana jest transpozycja do polskiego prawa postanowień dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu. Wskazać należy, że w ustawie o przeciwdziałaniu praniu pieniędzy znalazły się postanowienia odnoszące się do projektu zmian IV dyrektywy AML. Omawiane postanowienia dotyczą wirtualnych walut, które w ogóle nie są dostrzegane w obecnie obowiązującej treści IV dyrektywy AML. Zgodnie z art. 2 ust. 2 pkt 26 nowej ustawy o przeciwdziałaniu praniu pieniędzy[222], **waluta wirtualna** jest to cyfrowe odwzorowanie wartości, które nie jest:

a) prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,
b) międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
c) pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,
d) instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,
e) wekslem lub czekiem – oraz jest wymienialna w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywana lub przeniesiona albo może być przedmiotem handlu elektronicznego.

Definicja ta ściśle nawiązuje do definicji „waluty wirtualnej" zawartej w projekcie zmian IV dyrektywy AML. Z wykładni językowej polskiej definicji „wirtualnej waluty" wynika, że chodzi tu wyłącznie o pieniądz wkładowy (inaczej bankowy). Należy jednak zauważyć w tym miejscu, że jedynymi prawnymi środkami płatniczymi w Polsce są banknoty i monety opiewające na polskie złote. Należałoby zatem uznać, że mimo przyjętego ze względów raczej

[222] Dz.U. 2018 r., poz. 723.

praktycznych w orzecznictwie poglądu o skuteczności wykonania zobowiązania z liczby zapisanej w księdze rachunkowej banku (tzw. pieniądz bankowy), jedynym prawnym środkiem płatniczym w Polsce pozostaje moneta lub banknot opiewający na złote polskie. Powyższe rozważania każą powątpiewać w skuteczność wykonania zobowiązania przy użyciu tzw. kryptowalut. Wątpliwość ta zostałaby znacznie zmniejszona w wypadku przyjęcia definicji „waluty wirtualnej" zawartej w aktach unijnych. Całkowitym rozwiązaniem omawianego problemu jest preambuła jednej z nowszych wersji projektu V dyrektywy, z której wynika, że definicja „wirtualnej waluty" nie obejmuje „środków" (ang. *funds*) w rozumieniu dyrektywy PSD 2, czyli m.in. pieniądza bankowego (wkładowego). W preambule tej wersji projektu V dyrektywy wskazano ponadto, że wirtualnymi walutami w rozumieniu dyrektywy nie są: pieniądz elektroniczny (*electronic money*) w rozumieniu dyrektywy 2009/110/EC, wartość pieniężna przechowywana na instrumentach (*monetary value stored on instruments*), wyłączonych z zakresu przedmiotowego dyrektywy PSD 2 na podstawie jej art. 3(k) oraz 3(l), waluty używane wyłącznie w określonym środowisku danej gry (*in-games currencies, that can be used exclusively within the specific game environment*), pieniądze lokalne (*local currencies*, *complementary currencies*), jeżeli są używane w bardzo ograniczonych systemach (sieciach – *networks*), takich jak miasto lub region oraz wśród niewielkiej liczby użytkowników[223]. Powyższe rozważania zdają się mieć fundamentalne znaczenie dla poprawnego zdefiniowania waluty wirtualnej, jako takie powinny zostać transponowane jak najszybciej do prawa krajowego. Należy również zauważyć, że choć omawiana definicja nie dotyczy wyłącznie kryptowaluty, to ze względu na ich znaczną popularność, będzie ona wykorzystywana głównie w związku z nimi. Przykładowo, warunku definicji „waluty wirtualnej" nie spełniają tzw. tokeny, np. wyemitowane przy wykorzystaniu blockchainu systemu Ethereum. Zdefiniowanie waluty wirtualnej pozwala określić nowe podmioty obowiązane, którymi są według ustawy (art. 2 ust. 1 pkt 12) podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług w zakresie:

a) wymiany pomiędzy walutami wirtualnymi i środkami płatniczymi,
b) wymiany pomiędzy walutami wirtualnymi,

[223] http://www.witoldsrokosz.pl/pl/blog/legalna-definicja-waluty-wirtualnej-i-nowe-podmioty-obowiazane-prezydent-podpisal-nowa-ustawe [dostęp: 11.05.2018].

c) pośrednictwa w wymianie, o której mowa w lit. a lub b,
d) prowadzenia rachunków, o których mowa w ust. 2 pkt 17 lit. e ustawy, czyli prowadzenia w formie elektronicznej zbioru danych identyfikacyjnych zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany.

Wydaje się, że w wypadku punktu a) zasadna jest pewna korekta. W trosce o spójność z unijnymi regulacjami należy zobowiązać **podmiot prowadzący działalność gospodarczą w zakresie wymiany pomiędzy walutami wirtualnymi i prawnymi środkami płatniczymi.** Zawarcie w polskiej ustawie samego zwrotu „środki płatnicze" wydaje się nielogiczne. Warto również podkreślić, że ustawa nie zawiera definicji nowego terminu „środków płatniczych". Wydaje się, że jest to przeoczenie ustawodawcy, gdyż w uzasadnieniu projektu ustawy jest mowa tylko o wymianie walut wirtualnych na **prawne** środki płatnicze (powołując się na unijny projekt dyrektywy), nie ma natomiast wzmianki o wymianie walut wirtualnych na środki płatnicze. Należy podkreślić istnienie fundamentalnych różnic pomiędzy oboma terminami. **Prawne środki płatnicze są** rodzajem środków płatniczych. Dla przykładu – środkiem płatniczym może być złoto, regulowany pieniądz elektroniczny czy papiery wartościowe. Mimo że Polska ma pozostawioną dużą swobodę przy implementacji dyrektywy IV, to jednak tak istotna ingerencja w unijną konstrukcję wydaje się trudna do uzasadnienia. Należy jednak zauważyć, że ostateczna ocena polskiej regulacji może być dokonana dopiero po zakończeniu prac nad V dyrektywą AML. Warto także podkreślić, że zgodnie z nową ustawą o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu, aby stać się obowiązanym, wystarczy prowadzenie działalności gospodarczej w zakresie wymiany jednej kryptowaluty na inną kryptowalutę. Oprócz tego do zostania podmiotem obowiązanym wystarczy także świadczenie w ramach działalności gospodarczej usług w zakresie pośrednictwa w wymianie jednej kryptowaluty na inną lub też kryptowaluty na środek płatniczy. Ustawodawca nie wskazuje tu, o jakie pośrednictwo chodzi. W związku z powyższym uzasadnione jest szerokie rozumienie terminu „pośrednictwo", co ma niekorzystny wpływ np. na działalność osób, które w ramach wykonywania działalności gospodarczej prowadzą strony internetowe zawierające widgety dostarczane przez giełdy kryptowalut.

4.8. Rejestr transakcji walut wirtualnych

Głównym wyzwaniem stojącym przed wymiarem sprawiedliwości w związku z walutami wirtualnymi wydaje się powszechność korzystania z nich w związku z różnego rodzaju czynami przestępnymi. Istnieje wiele technik pozwalających utrudnić identyfikację stron biorących udział w transakcjach z udziałem walut wirtualnych. Rozwiązaniem służącym ułatwieniu identyfikacji stron dokonujących wspomnianych transakcji mogłoby być stworzenie rejestru transakcji z ich wykorzystaniem.

W innym miejscu zaproponowano wprowadzenie systemu licencji przyznawanych na prowadzenie działalności polegającej na świadczeniu usług w zakresie wymiany i pośredniczenia w wymianie walut wirtualnych. Wydaje się zasadne wprowadzenie w treści takiej licencji zakazu uczestniczenia w transakcjach, których strony nie są dostatecznie zidentyfikowane.

Należy również rozważyć zmianę ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu poprzez dodanie art. 72a o treści następującej: „podmioty wymienione w art. 2 ust. 1 pkt 12 są zobowiązane do przekazywania Generalnemu Inspektorowi informacji, o których mowa w art. 72 ust. 6, dotyczących czynności wymienionych w art. 2 ust. 1 pkt 12".

Zaproponowane rozwiązanie powinno znacząco ułatwić nadzór nad transakcjami dokonywanymi z udziałem walut wirtualnych oraz umożliwić identyfikację stron biorących w nich udział. Ma ona w zamyśle ułatwić wykrywanie sprawców przestępstw popełnianych z wykorzystaniem walut wirtualnych oraz znacząco utrudnić ukrywanie tożsamości stron transakcji. Stworzenie jednego zbioru danych dotyczących transakcji z wykorzystaniem walut wirtualnych, administrowanego przez Generalnego Inspektora lub inny w tym celu powołany organ, ułatwi znacząco kontrolę na rynkiem walut wirtualnych oraz utrudni wykorzystywanie tego rynku w działalności przestępczej.

ROZDZIAŁ PIĄTY

Zarządzanie ryzykiem w instytucjach finansowych

Nieustanny rozwój gospodarczy oraz związane z nim niebezpieczeństwa wymuszają na kierujących jednostkami finansowymi ciągłą czujność, analizę czynników związanych z ryzykiem oraz przyjęcie konkretnych rozwiązań i strategii zmierzających do minimalizowania go. Zauważyć należy, że już na początku lat dwutysięcznych proces oceny ryzyka stał się standardem oraz jednym z najważniejszych elementów okresowej oceny oraz kontroli w jednostkach sektora finansów. Charakter oraz kształt procedur kontroli ryzyka ulegał w kolejnych latach przemianom oraz rozszerzeniu o kolejne elementy, takie jak monitorowanie zarządzania ryzykiem w perspektywie realizacji i osiągania celów i zadań konkretnych jednostek. Rozwój metod analizy ryzyka towarzyszącego działalności finansowej zaowocował wytworzeniem się procesów i procedur zarządzania ryzykiem oraz odpowiedniego reagowania. Wypracowane standardy oraz rozwiązania powinny się upowszechnić, stając się częścią systemu kontroli zarządczej, również w jednostkach sektora finansów publicznych (JSFP). Jak wskazują przedstawiciele doktryny[224], nie wypracowano dotychczas ujednoliconej, wspólnej wszystkim jednostkom procedury i strategii prowadzenia kontroli zarządczej oraz metod zarządzania ryzykiem. Zazwyczaj wszelkie próby takiego działania z uwagi na pionierski charakter cechują się pewną niedoskonałością.

[224] E.I. Szczepankiewicz, A. Wójtowicz, *Model rejestru ryzyka w jednostkach sektora finansów publicznych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2015, nr 864.

5.1. Źródła ryzyka, analizy i zarządzania ryzykiem

Zauważyć należy, że wszelkie zdarzenia, mogące w jakiś sposób negatywnie wpłynąć lub przeszkodzić w osiągnięciu celów i zadań realizowanych przez JSFP, określić można mianem ryzyka. Konieczność zarządzania ryzykiem w omawianych jednostkach wynika z obowiązku ustawowego wyrażonego w ustawie o finansach publicznych oraz z komunikatów Ministra Finansów[225]. Zgodnie ze słownikową definicją ryzyko rozumieć należy jako cechę działania, którego wynik jest niepewny lub nieznany. Pod pojęciem tym jednak, w kontekście działalności podmiotów na rynku finansowym, rozumieć należy takie stany faktyczne jak: możliwość wystąpienia zdarzenia nieprzewidzianego, stan zagrożenia, a także możliwość poniesienia straty finansowej, prawnej lub wizerunkowej. W ramach analizy ryzyka możliwe jest określenie prawdopodobieństwa wystąpienia zjawisk i stanów o charakterze losowym i operacyjnym. Zauważyć należy, że – jak wskazuje praktyka – ryzyko związane z wystąpieniem niekorzystnych i niezaplanowanych zdarzeń jest możliwe do oszacowania. Taka analiza prawdopodobieństwa wskazuje, że możliwe jest zarządzanie ryzykiem w celu jego ograniczenia. Przez pojęcie „zarządzania ryzykiem" w kontekście instytucji finansowych rozumieć należy więc ogół działań mających na celu: identyfikację, analizę, ocenę i hierarchizację ryzyka, a także reakcję na ryzyko, kontrolę i monitoring ryzyka[226]. Kierownictwo JSFP zobligowane jest do przeprowadzania analiz mających na celu identyfikację źródła i czynników ryzyka we wszystkich aspektach i obszarach funkcjonowania podległej mu jednostki. Analizie powinien podlegać całokształt procesów zachodzących wewnątrz, na zewnątrz jednostki oraz wszelkich czynników bezpośrednio lub pośrednio wpływających na sytuację danego podmiotu finansowego. Jako wewnętrzne czynniki analizie podlegać muszą: procesy organizacyjne i zarządcze, finanse, środowisko informatyczne i wszystkie czynniki specyficzne dla rodzaju realizowanych zadań publicznych i rodzaju działalności. Za zewnętrzne źródła ryzyka określić należy między innymi: otoczenie prawne i ekonomiczne, infrastrukturę,

[225] Komunikat nr 6 Ministra Finansów z dnia 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem.

[226] Komunikat nr 23..., 2009; Komunikat nr 6..., 2012.

klientów, wykonawców itp. Zauważa się, że zarządzanie ryzykiem powinno być uwzględnione w procesie realizacji zadań danej jednostki. Musi ono swym zakresem obejmować wszystkie cele i zadania, a także obszary działalności jednostki. W tym kontekście celem podejmowanych działań jest identyfikacja czynników i zdarzeń mogących wywierać wpływ na jednostkę, a także skutków ich wystąpienia oraz utrzymanie ryzyka na określonym poziomie umożliwiającym realizację zadań jednostki. Wskazać więc należy, że podstawowym warunkiem prawidłowej oceny ryzyka jest precyzyjne ustalenie celów oraz zadań na dany rok dla konkretnej jednostki. Ocena ta powinna być kompleksowa oraz brać pod uwagę wiedzę o strukturze jednostki oraz jej zadaniach, także wiedzę na temat stanu i przebiegu współpracy z innymi jednostkami, nadrzędnymi oraz podrzędnymi. Musi również dostosowywać nieustannie poziom ryzyka do swych potrzeb oraz możliwości. Wiedza na temat dopuszczalnego ryzyka powinna być powszechna wśród pracowników. Kierownictwo jednostek powinno wspólnie z pracownikami działać na rzecz skutecznego zarządzania ryzykiem. Fundamentalne znaczenie w kontekście prawidłowego określenia wartości ryzyka mają sposoby rozpoznawania wewnętrznych i zewnętrznych czynników ryzyka oraz wskazanie zakresu ich oddziaływania. Zauważyć jednak należy, że nie opracowano jeszcze uniwersalnej metody pozwalającej na identyfikację ryzyka w JSFP. Kierownictwa jednostek przygotowują własne strategie oraz metody, zgodne z nabytym przez nich doświadczeniem, a także specyfiką działania danej jednostki. Ocena konkretnych zagrożeń zależy od charakteru ryzyka, warunków analizy i dostępnych w momencie analizy informacji. W praktyce jednostek stosuje się wiele różnych metod identyfikacji ryzyka lub ich kombinacje. Mającą największe znaczenie i najczęściej stosowaną metodą identyfikacji ryzyka jest analiza danych historycznych zgromadzonych w jednostce. Wadą tej metody jest jednak ograniczenie analizy wyłącznie do zjawisk oraz ryzyka występujących w przeszłości. Nie dostrzega więc nowych rodzajów ryzyka, a w sytuacji jednostek nowo powstałych nie daje żadnych rezultatów w związku z brakiem historii jako punktu odniesienia. Wiele jednostek identyfikuje ryzyko, wykorzystując do tego celu różnego rodzaju ankiety, kwestionariusze oraz inne tego typu narzędzia. Niezależnie od wykorzystanych metod analiza ryzyka powinna zmierzać do ustalenia istotności ryzyka, czyli określenia prawdopodobieństwa wystąpienia i skutków, które potencjalnie może ono wywołać. Na potrzeby

takiej analizy przyjmuje się określone skale oceny ryzyka (np. 3- lub 5-stopniową). Metodę określenia istotności ryzyka, która będzie dostosowana do potrzeb i celów jednostki. Wynikiem oszacowania ryzyka powinna być lista ewentualnych skutków zniszczenia ryzyka opracowana z uwzględnieniem istotności ryzyka (np. ryzyko niskie, średnie, wysokie). Ryzyko opisać można matematycznie jako iloczyn prawdopodobieństwa jego zaistnienia i wielkości skutków, jakie może ono wywołać. Wielkość tak określonego ryzyka można w ramach procesu analizy przedstawiać za pomocą wykresów lub na tzw. mapie ryzyka. Po zanalizowaniu ryzyka i ustaleniu poziomu akceptowalnego tworzy się listę czynników sprzyjających oraz decyduje o podjęciu wobec nich odpowiednich działań oraz o dalszej ich analizie[227].

Efektem analizy ryzyka powinno być podjęcie działań zmierzających do zapobiegania zjawiskom, stwarzającym istotne zagrożenie dla realizacji celów oraz zadań jednostki. W odniesieniu do czynników i obszarów ryzyka, które oceniono jako istotne, zwykle podejmuje się działania w postaci:

- tolerowanie zjawiska;
- przeciwdziałania;
- przeniesienie ryzyka poprzez ubezpieczenie itp.;
- wycofania się z danego przedsięwzięcia.

Kierownictwo jednostki powinno świadomie reagować na występujące ryzyko, opierając swe decyzje, podejmowane w ramach zarządzania ryzykiem, na podstawie przeprowadzonych analiz, badań i ekspertyz. Powinno również brać pod uwagę koszty podjęcia określonych działań. Doświadczenie nabywane w trakcie tego procesu powinno być nieustannie weryfikowane w celu wyciągania wniosków oraz aktualizowania strategii postępowania z ryzykiem. Podczas tej weryfikacji należy uwzględniać zmiany zachodzące w jednostce i jej otoczeniu. Nie budzi wątpliwości, że aby kierownictwo jednostek sektora finansów publicznych mogło sprawnie zarządzać ryzykiem, powinno właściwie skonstruować rejestr ryzyka, będący narzędziem pozwalającym uzyskać rzetelną informację do celów skutecznego zarządzania ryzykiem[228].

[227] T.T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2008.

[228] E.I. Szczepankiewicz, A. Wójtowicz, *op. cit.*

5.2. Ryzyko związane z prowadzeniem działalności gospodarczej

Ryzyko wiążące się z prowadzeniem działalności gospodarczej, z inwestycjami oraz działalnością instytucji finansowych jest częstym przedmiotem analiz.

Powszechnie w ramach analizy wyróżnia się trzy typy ryzyka: zewnętrzne, wewnętrzne oraz losowe[229].

Ryzyka zewnętrzne mają związek ze zmianami politycznymi, społecznymi, demograficznymi, zmianami prawa i regulacji, ekonomicznymi procesami, konkurencją, dostępnością do rynków, postępem technologicznym, decyzjami akcjonariuszy, zachowaniem kontrahentów, stanem innych prowadzonych inwestycji.

Wewnętrzne ryzyko strategiczne objawia się zazwyczaj w sytuacji niepowodzenia utrzymania udziału w rynku, w identyfikacji potrzeb klientów, realizacji strategii wejścia na rynek, fuzji, alokacji działalności, nieskutecznego kierownictwa, niedostosowania do potrzeb struktur organizacyjnych oraz możliwości utraty dobrego wizerunku wskutek błędnych zachowań.

Wewnętrzne ryzyko finansowe wiązać należy z planowaniem finansowym, dostępnością źródeł finansowania, kredytami, płatnościami, płynnością finansową, inwestycjami, stopą procentową, inflacją, karami umownymi, stratami itp.

Ryzyko operacyjne jest złożonym zjawiskiem. Część doktryny określa je jako efekt niewystarczającej kontroli, błędów ludzkich lub awarii systemów informatycznych. W dziedzinie błędów ludzkich występuje zazwyczaj pod postacią niedoświadczenia, niekompetencji oraz korupcji. Inaczej definiuje się je jako: ryzyko poniesienia pośrednich lub bezpośrednich strat, związanych z niewłaściwie prowadzonymi lub błędnymi wewnętrznymi procesami, osobami czy systemami, albo wiążących się ze zdarzeniami zewnętrznymi[230].

[229] *Ibidem.*

[230] P. Matkowski, *Zarządzanie ryzykiem operacyjnym*, Kraków 2006.

Tabela 3. Klasyfikacja ryzyka operacyjnego.

Obszary ryzyka	Zagrożenia, zdarzenia i czynności lub zaniechanie działań związanych z:
Konkurencyjność	pozyskaniem nowych i utrzymaniem obecnych klientów, satysfakcją klientów, zyskownością klientów, czasem operacji, rozwojem produktów, utratą wartości marki
Kontrakty	zawieraniem umów (ryzyko prawne, dodatkowych kosztów, nieprzestrzegania harmonogramu prac, niepełne specyfikacje), niedotrzymaniem warunków umów, zaniechaniem czynności podczas trwania inwestycji lub końcowego odbioru robót
Zarządzanie procesami wewnętrznymi	realizacją, dostawami, utrzymywaniem zapasów, logistyką i dystrybucją, efektywnością i jakością procesów, wyceną produktów, błędami serwisu, realizacją projektów i inwestycji
Prowadzenie działalności zgodnie z regulacjami	niestosowaniem się do przepisów prawa, standardów, regulacji dotyczących danej instytucji, wypełnianiem norm sektorowych, branżowych, środowiskowych i innych, balansowanie z wykorzystaniem luk prawnych
Ochrona zasobów i bezpieczeństwo informacji	zniszczeniem, utratą, nieuprawnionym wykorzystaniem zasobów rzeczowych, zarządzaniem licencjami, innowacjami i środowiskiem IT, ciągłością działania systemów informatycznych, awariami infrastruktury IT
Kontrola wewnętrzna	adekwatnością wewnętrznych regulacji i procedur, prowadzeniem dokumentacji, wiarygodną sprawozdawczością, podziałem uprawnień i odpowiedzialnością, ochroną przed defraudacjami i aktami przestępczymi
Ludzki	czynnikami wpływającymi na zdrowie i bezpieczeństwo pracowników i klientów, utratą kluczowych specjalistów lub kompetencyjnej kadry kierowniczej

Źródło: na podstawie opracowania: E.I. Szczepankiewicz, *Wykorzystanie punktowej metody oszacowania ryzyka operacyjnego w instytucjach finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 298.

Ryzyka losowe wiążą się z wystąpieniem niezależnych od instytucji zjawisk, podobnych do pożarów, powodzi, katastrof budowlanych itp. Ryzyka te mogą być też w pewnych sytuacjach wywołane przez czynniki wewnętrzne, wynikające z niedopełnienia przepisów, wewnętrznych procedur lub błędów personelu.

5.3. Sposoby reagowania na ryzyko

Jak już wskazywano, zarządzanie ryzykiem operacyjnym w instytucji finansowej powinno być stałym działaniem realizowanym przy współpracy kierownictwa oraz pracowników[231]. Modelowo prawidłowy proces zarządzania ryzykiem w instytucji finansowej powinien wyglądać w następujący sposób:

[231] K. Jajuga, *Zarządzanie ryzykiem*, Warszawa 2018.

- ustalenie celów strategicznych instytucji i celów operacyjnych dla poszczególnych komórek organizacyjnych,
- opisanie procesów biznesowych i wskazanie ich właścicieli,
- identyfikacja czynników oraz obszarów ryzyka w odniesieniu do procesów, systemów i jednostek organizacyjnych,
- analiza i oszacowanie ryzyka w powyższych obszarach (określenie przyczyn, częstotliwości i siły wpływu skutków na instytucję),
- określenie poziomu ryzyka akceptowanego przez kierownictwo,
- segregacja i hierarchizacja ryzyka według istotności,
- określenie strategii postępowania z ryzykiem w obszarach,
- zastosowanie ustalonych narzędzi redukcji i kontroli ryzyka,
- monitorowanie poziomu ryzyka i efektywności redukcji ryzyka,
- raportowanie wyników o skuteczności zarządzania ryzykiem,
- ocena skuteczności i wprowadzanie działań korygujących.

Zazwyczaj w ramach zarządzania ryzykiem używa się wielu metod i sposobów analizy ryzyka[232]. Do najczęściej stosowanych należą: odpowiednie metody ilościowe, statystyczne, a także rzadziej narzędzia informatyczne, wspomagające wykorzystanie metod ilościowych i jakościowych. Podstawowym celem wszelkich analiz ryzyka jest wskazanie zagrożeń istotnych i nieistotnych. Wobec ryzyk istotnych należy podjąć natychmiastowe działania. Podczas ustalenia istotności ryzyka należy brać po uwagę takie czynniki, jak[233]:

- znaczenie finansowe strat, czyli ich wpływ na wynik finansowy,
- znaczenie skutków ryzyka dla wizerunku,
- znaczenie dla wypełniania obowiązków ustawowych oraz wewnętrznych wytycznych,
- koszt działań ochronnych.

[232] K. Maderak, *Ewolucja metod kwantyfikacji ryzyka*, „Bank" 2010, nr 9.
[233] E.I. Szczepankiewicz, A. Wójtowicz, *op. cit.*

Tabela 4. Czynniki wpływające na ustalenie istotności ryzyka.

Wpływ strat na wynik finansowy	Ryzyko istotne dla instytucji	Znaczenie dla wypełniania obowiązków ustawowych oraz wewnętrznych wytycznych
Koszty działań ochronnych		Znaczenie dla wizerunku

Źródło: na podstawie opracowania: E.I. Szczepankiewicz, *Wykorzystanie punktowej metody oszacowania ryzyka operacyjnego w instytucjach finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 298.

Określenie poziomu ryzyka pozwala na podejmowanie decyzji dotyczących działań w związku ryzykiem oraz stanowi podstawę projektowania odpowiednich procedur kontrolnych. Ma to, jak już wskazywano, fundamentalne znaczenie dla jakości zarządzania instytucją.

Powszechnie wyróżnia się pięć sposobów reakcji na ryzyko. Scharakteryzowano je w poniższej tabeli.

Tabela 5. Strategie postępowania z ryzykiem w instytucji finansowej.

Strategia	Charakterystyka strategii
Redukcja i monitorowanie ryzyka	zapobieganie wystąpieniu ryzyka lub zmniejszenie jego skutków poprzez zastosowanie takich mechanizmów, jak: systematyczna ocena i monitorowanie ryzyka, stosowanie technicznych i organizacyjnych środków ochrony zasobów, wdrożenie procedur kontrolnych, szkolenie personelu, wprowadzenie systemów jakości, ocena dostawców usług zewnętrznych, zabezpieczenia prawne wykonania umów i inne mechanizmy zapobiegawcze, nakazowe, korygujące, wykrywające
Akceptowanie określonego poziomu ryzyka (ryzyko akceptowalne)	to decyzja o braku reakcji na ryzyko lub o jego tolerowaniu; dotyczy to przypadków, gdy zarządzający akceptuje ryzyko: o niskim prawdopodobieństwie i skutkach jego wystąpienia (ryzyko nieznaczne); dana działalność niesie za sobą potencjalnie wyższą wartość dodaną niż koszt stosowanych środków ochrony; powstało ryzyko rezydualne (pozostałe), którego nie można całkowicie wyeliminować środkami ochrony; tworzy się plany awaryjne, które stanowią zabezpieczenie w momencie wzrostu ryzyka, ryzyko jest monitorowane
Dywersyfikacja ryzyka	poprzez rozproszenie ryzyka, np. *outsourcing* obsługi działań, w których brakuje kompetencji w instytucji, a także: zmniejszenie koncentracji ryzyka IT związanego z kluczowymi dostawcami sprzętu, zabezpieczeń, usług serwisowych itp.
Transfer ryzyka	poprzez przeniesienie na inne podmioty poprzez np. ubezpieczenie: od zdarzeń losowych, baz danych, sprzętu informatycznego, projektu

Strategia	Charakterystyka strategii
Unikanie ryzyka	poprzez rezygnację z procesu lub redefinicję procesu, w taki sposób, aby wyeliminować lub zmniejszyć ryzyko nieodzowne w działalności, metodami organizacyjnymi (np. podział uprawnień użytkowników systemów informatycznych), metodami technicznymi (np. zakup dobrej jakości sprzętu i systemów, zabezpieczenie techniczne serwerowi) lub rezygnacja z prowadzenia projektu narażonego na duże ryzyko niepowodzenia

Źródło: na podstawie opracowania: E.I. Szczepankiewicz, *Wykorzystanie punktowej metody oszacowania ryzyka operacyjnego w instytucjach finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 298.

Wydaje się, że skutki oraz prawdopodobieństwo wystąpienia niekorzystnego zjawiska to kluczowe czynniki doboru odpowiedniej metody zarządzania ryzykiem. Na poniższej tabeli przedstawiono najpowszechniejsze sposoby postępowania z ryzykiem ze względu na te dwa czynniki.

Tabela 6. Strategie postępowania z ryzykiem w instytucji finansowej ze względu na stopień szkodliwości i prawdopodobieństwo wystąpienia ryzyka.

Prawdopodobieństwo wystąpienia ryzyka				
	Wysokie	Ciągłe monitorowanie i weryfikacja ryzyka, redukcja ryzyka i transfer ryzyka pozostałego	Ciągłe monitorowanie i weryfikacja ryzyka, unikanie ryzyka poprzez reorganizację lub transfer ryzyka (ubezpieczenie, reasekuracja, *outsourcing*)	Unikanie ryzyka poprzez rezygnację z procesu lub działania, zapobieganie ryzyku u źródła
	Średnie	Ciągłe monitorowanie i weryfikacja ryzyka, redukcja ryzyka i akceptacja ryzyka pozostałego	Ciągłe monitorowanie i weryfikacja ryzyka, redukcja ryzyka lub transfer ryzyka	Ciągłe monitorowanie i weryfikacja ryzyka, redukcja ryzyka i transfer ryzyka pozostałego (ubezpieczenie, reasekuracja, *outsourcing*)
	Niskie	Brak reakcji na ryzyko, akceptacja, tolerowanie ryzyka na określonym poziomie, minimalne monitorowanie i okresowa weryfikacja	Ciągłe monitorowanie ryzyka i okresowa weryfikacja, akceptacja ryzyka lub tolerowanie ryzyka na określonym poziomie	
		Niski	Średni	Wysoki
		Stopień szkodliwości		

Źródło: na podstawie opracowania: E.I. Szczepankiewicz, *Wykorzystanie punktowej metody oszacowania ryzyka operacyjnego w instytucjach finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 298.

Równie ważna, co realizacja danego sposobu postępowania z ryzykiem, jest ciągła ocena i badanie skuteczności strategii[234]. Badanie jakości zarządzania

[234] L. Szyszko, *Finanse przedsiębiorstwa*, Warszawa 2007.

ryzykiem w instytucjach finansowych powinno się odbywać w ramach funkcjonujących w nich odpowiednich systemów kontroli wewnętrznej. Ryzyka z działalności w rzeczywistości gospodarczej i finansowej nie da się w całości wyeliminować. Możliwe jest jedynie minimalizowanie w taki sposób, aby nie przeszkadzało w stabilnym i prawidłowym funkcjonowaniu.

Podkreślić należy, że skuteczne zarządzanie ryzykiem jest procesem trudnym i złożonym. Dzieje się tak z uwagi na fakt wyjątkowości sytuacji każdej instytucji finansowej oraz różnorodność oddziałujących na nie zjawisk. W związku z tym wydaje się, że możliwe do sformułowania są jedynie pewne ogólne zalecenia na temat sposobów zarządzania ryzykiem. Zalecenia te powinny prowadzić do wykształcania się powszechnych stadardów, nawyków oraz procedur dotyczących postępowania z ryzykiem. Wskazać należy, że za wyjątkowo istotny czynnik oddziałujący na jakość przebiegu procesu zarządzania ryzykiem uznać należy: posiadanie odpowiedniego doświadczenia oraz kompetencji przez zarząd i kierownictwo, a także odpowiednią konsekwencję w działaniu. Niezwykle ważne z perspektywy zarządzania ryzykiem jest współdziałanie pracowników oraz kierownictwa w realizacji ustalonych celów, przestrzeganiu procedur wewnętrznych oraz kształtowaniu pozytywnej kultury pracy. Zarząd instytucji finansowej musi nieustannie ewoluować i doskonalić system zarządzania ryzykiem. Musi także w sposób ciągły oceniać skuteczność realizowanych procedur oraz standardów kontroli zapobiegającej występowaniu zjawisk szkodliwych oraz skuteczności kontroli realizowanych zadań przez kierownictwo operacyjne w poszczególnych pionach organizacyjnych.

5.4. Zarządzanie ryzykiem w instytucjach finansowych a stopień nasilenia przestępczości. Nowe rodzaje zarządzania ryzykiem w instytucjach finansowych

Instytucje finansowe, definiowane jako podmioty prowadzące działalność na rynku finansowym, formułują własne cele ekonomiczne oraz podejmują działania zmierzające do ich realizacji. Głównym celem każdego podmiotu biorącego udział w grze rynkowej, a zatem i instytucji finansowej, jest wykazanie zysków oraz wspomnożenie aktywów własnych. Osiąganie zysku w ramach operacji na rynku finansowym wiąże się z tzw. ryzykiem operacyjnym. Przez

określenie „ryzyko" rozumie się na ogół taki stan rzeczy, gdy istnieje szansa ziszczenia się zdarzenia, które wpłynie negatywnie na sytuację podmiotu[235]. Organy instytucji finansowych odpowiedzialne za podejmowanie decyzji są świadome istnienia różnych rodzajów ryzyka związanych z działalnością instytucji finansowej. Celem jego ograniczenia wdrażają programy umożliwiające przeanalizowanie, a także ograniczenie prawdopodobieństwa zrealizowania się ryzyka oraz dolegliwości jego skutków. Opisane działanie zmierzające do ograniczenia ryzyka określa się w doktrynie mianem „zarządzania ryzykiem"[236]. Przedmiotem niniejszej analizy jest kwestia bezpieczeństwa instytucji finansowych, ryzyka wystąpienia przestępstw finansowych oraz związku pomiędzy procesami zarządzania ryzykiem a zagrożeniem przestępczością finansową.

5.5. Ryzyko w działalności instytucji finansowych

Bezpieczeństwo instytucji finansowych jest ściśle powiązane z zagadnieniem ryzyka. Poprawnemu wykonywaniu swoich zadań przez instytucję finansową zagraża wiele negatywnych zjawisk, których analiza prowadzi do wniosku, że w ramach swojej działalności instytucja finansowa jest narażona na różnorodne rodzaje ryzyka, np. ryzyko płynności, ryzyko rynkowe, ryzyko kredytowe, ryzyko operacyjne, ryzyko kapitałowe, ryzyko ubezpieczenia. Jednakże możliwe jest świadome ograniczanie ryzyka w ramach procedur zarządzania instytucją finansową. To właśnie wskutek prawidłowo prowadzonego procesu zarządzania oraz odpowiednio działającej kadry menadżerskiej możliwe jest takie ukształtowanie struktury instytucji oraz sposobów realizacji zamierzonych celów, który pozwala w jak największym stopniu ograniczać ryzyko strat oraz zwiększać prawdopodobieństwo zysków[237]. W kontekście powyższej refleksji uprawnione wydaje się stwierdzenie, że mianem zarządu instytucją finansową określić można w istocie proces zarządzania ryzykiem, którego celem jest zapewnienie sprawnego funkcjonowania instytucji, nawet w warunkach nietypowych. Podstawowym celem jest więc zapewnienie możliwie

[235] S. Bereza, *Zarządzanie ryzykiem bankowym*, Warszawa 1992.
[236] J. Krasodomska, *Zarządzanie ryzykiem operacyjnym w bankach*, Warszawa 2008.
[237] M. Iwanicz-Drozdowska, *Zarządzanie finansowe bankiem*, Warszawa 2005.

bezpiecznego funkcjonowania. Bezpieczeństwo instytucji można więc w tym kontekście rozumieć przez pryzmat uwarunkowań działalności, celu działania oraz kryterium oceny sposobu funkcjonowania.

Zasadne wydaje się dla pełniejszej analizy omawianego zagadnienia zbadanie kwestii ryzyka związanego z działalnością instytucji finansowych, tj. ryzyka operacyjnego.

Mnogość ryzyka podyktowana bywa zwykle zmiennym charakterem rzeczywistości gospodarczej oraz związaną z tym niepewnością. W rozważaniach doktryny zauważyć można w ostatnim czasie szczególne zainteresowanie kwestią ryzyka operacyjnego. Wydaje się, iż jest to podyktowane wagą wynikających z niego skutków dla podejmowanej działalności. Ponadto wpływ na obranie tego kierunku badań ma rozwój technologiczny, różnego rodzaju przekształcenia i fuzje, *e-commerce*, a także różnorodna działalność banków, która może w efekcie prowadzić do powstawania strat finansowych[238].

Przemiany zachodzące w rzeczywistości rynkowej, w tym rozwój technologiczny, mnogość i skomplikowanie usług bankowych, przemiany prawne oraz procesy globalizacyjne, niejako wskazują na konieczność zbadania kwestii ryzyka operacyjnego. Ryzyko to, mimo iż będące zjawiskiem powszechnie znanym, w związku z rozwojem zyskało w ostatnim czasie na szczególnym znaczeniu.

Występujące w latach w latach 90. XX wieku zjawiska strat operacyjnych, związane z popełnianymi błędami w obszarze kontroli lub błędnie określonego charakteru struktury organizacyjnej banków o dużej renomie, doprowadziły instytucje nadzoru finansowego do wprowadzenia konkretnych rozwiązań prawnych w zakresie zarządzania ryzykiem operacyjnym. Znaczącym przejawem zmian zachodzących w podejściu do kwestii ryzyka operacyjnego okazało się ujęcie tego rodzaju ryzyka w Nowej Umowie Kapitałowej. Zauważyć należy, że również Bazylejski Komitet ds. Nadzoru Bankowego opracował w 2003 r. „Zasady Dobrej Praktyki w Zakresie Zarządzania i Nadzoru nad Ryzykiem Operacyjnym"[239]. Dokument ten pozwolił Komisji Nadzoru

[238] J. Jakóbczak, *Współczesne tendencje w zarządzaniu ryzykiem operacyjnym*, „Nasz Rynek Kapitałowy" 2003, nr 5.

[239] I. Majer, *Podejście standardowe w Nowej Umowie Kapitałowej a procykliczność działalności kredytowej*, „Master of Business Administration. Pismo Wyższej Szkoły Przedsiębiorczości i Zarządzania im. L. Koźmińskiego i Międzynarodowej Szkoły Zarządzania" 2007, nr 2.

Bankowego na sporządzenie w 2013 r. tzw. „Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach".

Zgodnie z zaleceniami „Rekomendacji M" przez ryzyko operacyjne powinno się rozumieć ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub ze zdarzeń zewnętrznych. Ponadto ryzyko to zawiera w sobie również pojęcie „ryzyka prawnego", wyłączone z niego jest ryzyko strategiczne i ryzyko reputacji.

„Rekomendacja M"[240] proponuje również podział ryzyka operacyjnego na siedem podtypów.

1. Oszustwa wewnętrzne – oszustwa pracowników banku, oszustwa kredytowe, oszustwa czekowe, łapówkarstwo, fałszowanie sprawozdawczości wewnętrznej, niszczenie aktywów.

2. Oszustwa zewnętrzne – oszustwa wykonywane przez osoby trzecie np.: kradzież, rabunek, włamania, ataki hakerskie.

3. Praktyka kadrowa i bezpieczeństwo pracy – łamanie przez władze instytucji regulacji prawa pracy oraz BHP, a także roszczenia pracownicze.

4. Klienci, produkty i praktyka biznesowa – negatywne zjawiska prowadzące do spadku zaufania klientów, ujawniania informacji wrażliwych dotyczących klientów, agresywnej strategii handlowej, niedozwolonych transakcji na rachunkach bankowych klientów oraz wadliwe konstrukcje umów regulaminów itp.

5. Uszkodzenia aktywów – oddziaływanie siły wyższej oraz innych podobnych zjawisk prowadzących do utraty powierzonych aktywów.

6. Zakłócenia działalności i błędy systemów – np. nieprawidłowe działanie sprzętu, błędy oprogramowania, problemy telekomunikacyjne, itp. prowadzące do zakłócenia pracy instytucji.

7. Dokonywanie transakcji, dostawa oraz zarządzanie procesami – błędy w trakcie wprowadzania danych do systemu, wykonania, rozliczania i obsługi transakcji, wadliwe prowadzenie dokumentacji klientów banku, niewłaściwe zarządzanie rachunkami klientów.

[240] https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_M_8_01_2013_uchwala_8_33017.pdf [dostęp: 11.05.2019].

Analiza ryzyka operacyjnego pozwala wskazać cechy charakterystyczne, odróżniające ten konkretny rodzaj ryzyka od pozostałych[241]:

- ziszczenie się ryzyka operacyjnego w każdym wypadku owocuje negatywnymi skutkami dla instytucji finansowej,
- każde działanie podejmowane przez instytucję finansową wiąże się z ryzykiem operacyjnym,
- ryzyko operacyjne można jedynie ograniczyć. Nie jest możliwa jego całkowita eliminacja,
- z uwagi na zróżnicowanie sytuacji, w których mamy do czynienia z tym rodzajem ryzyka, jego zbadanie jest niezwykle problematyczne.

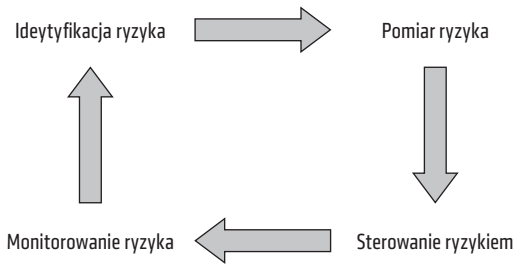
Należy zauważyć, że przyczyną niemożliwości eliminacji ryzyka operacyjnego jest tzw. przestępczość finansowa. Zdarzenia o charakterze przestępnym, wymierzone w interesy instytucji finansowych, można podzielić według kryterium przynależności podmiotu sprawczego do struktury organizacyjnej instytucji finansowej. Zastosowanie wskazanego kryterium pozwala na wyróżnienie dwóch kategorii przestępstw finansowych: zewnętrznych (kradzieże i wyłudzenia środków finansowych oraz danych, oszustwa zewnętrzne) oraz wewnętrznych (defraudacje dokonywane przez pracowników oraz różnego rodzaju oszustwa wewnętrzne)[242]. Trudność całkowitego ograniczenia ryzyka operacyjnego, ściślej ryzyka przestępstw finansowych, wynika z faktu, że są one efektem świadomego działania ludzi nakierowanego na szkodę instytucji finansowej oraz zysk własny. Z punktu widzenia niniejszego opracowania bezcelowe wydaje się prowadzenie filozoficznych rozważań na temat kondycji ludzkiego ducha oraz zagadnienia chciwości – wystarczy powiedzieć, że chęć osiągnięcia zysku pozostanie motywem przestępstw finansowych w przewidywalnej przyszłości, niezależnie od jakości zarządzania ryzykiem operacyjnym w instytucjach finansowych. Zadaniem odpowiedzialnego zarządu pozostaje natomiast przygotowanie konkretnych procedur służących ograniczeniu wspomnianego ryzyka: zapewnienie stałej kontroli czynności podejmowanych przez pracowników, umożliwienie sprawnej wymiany informacji pomiędzy poszczególnymi organami instytucji finansowych oraz szybkiej reakcji

[241] K. Raczkowski, *Bezpieczeństwo ekonomiczne obrotu gospodarczego. Ekonomia. Prawo. Zarządzanie*, Warszawa 2014.

[242] T.T. Kaczmarek, *op. cit.*

w związku z wykrytymi nieprawidłowościami, a także ograniczanie dolegliwości skutków zdarzeń o charakterze przestępczym poprzez transfer ryzyka.

Rysunek 1. Zarządzanie ryzykiem.



Należy zauważyć, że najistotniejszym etapem procesu zarządzania ryzykiem przez instytucję pozostaje jego identyfikacja oraz określenie prawdopodobieństwa jego ziszczenia. To właśnie trafna analiza grożącego ryzyka umożliwia podjęcie kroków w celu jego ograniczenia. Analiza ryzyka powinna zawsze skupiać się na ocenie prawdopodobieństwa ziszczenia się go oraz na ustaleniu dolegliwości jego ewentualnych skutków. Wyliczeniu wielkości grożącego ryzyka służy poniższy wzór[243]:

$$\mathbf{R = P \times S}$$

gdzie:

R – wielkość oczekiwanej straty związanej z danym ryzykiem,

P – prawdopodobieństwo wystąpienia rozpatrywanego zdarzenia (częstotliwość strat),

S – skutek (oddziaływanie), gdy wystąpi rozpatrywane zdarzenie (poziom strat).

Prawdopodobieństwo (P) można w niektórych wypadkach obliczyć, wykorzystując dostępne dane – w innych natomiast może jedynie być określone na podstawie intuicji badacza. Negatywnym skutkiem ziszczenia się ryzyka może być utrata środków finansowych, wystąpienie niekorzystnych skutków prawnych oraz straty wizerunkowe danej instytucji. Przypisanie

[243] E.L. Szczepankiewicz, *Wykorzystanie punktowej metody oszacowania ryzyka operacyjnego w instytucjach finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 298.

odpowiednich wartości prawdopodobieństwu ziszczenia się ryzyka oraz dolegliwości jego ewentualnych skutków pozwala skonstruować macierz ryzyka ułatwiającą jego ocenę oraz sformułowanie odpowiedniego planu zarządzania nim. Należy dodatkowo zauważyć, że im bardziej rozbudowaną opracuje się macierz, tym dokładniejszy uzyskamy pomiar oraz tym bardziej złożony program zarządzania ryzykiem pozwoli ona przygotować[244].

Przyjmuje się, że operacje o najniższym stopniu ryzyka nie wymagają żadnych działań zmierzających do jego ograniczenia. Jak już bowiem wspomniano, ryzyko jest nieodłącznym elementem gry rynkowej i nie jest możliwe jego całkowite wyeliminowanie. Dopiero tzw. średnie ryzyko wymaga podjęcia odpowiednich kroków mających na celu obniżenie szansy jego wystąpienia oraz systematycznego monitorowania. Zdarzenia o najwyższym stopniu ryzyka wymagają natomiast podjęcia natychmiastowych działań interwencyjnych[245]. Interpretacji macierzy ryzyka może posłużyć tabela:

Tabela 5. Przykładowa interpretacja pięciostopniowej macierzy ryzyka.

Punkty w skali 1–5	Wartość % dla skali 1–5	Opis prawdopodobieństwa	Przykładowa interpretacja prawdopodobieństwa ryzyka
1.	1–19%	Małe	Prawdopodobieństwo małe, jeśli istnieje mała szansa na wystąpienie ryzyka lub w ostatnich pięciu latach ono nie występowało
2.	20–39%	Umiarkowane	Prawdopodobieństwo umiarkowane, jeśli ryzyko występuje rzadko, np. raz na trzy lata
3.	40–59%	Wysokie	Prawdopodobieństwo wysokie, jeśli ryzyko pojawia się dość często, np. raz na dwa lata
4.	60–79%	Bardzo wysokie	Prawdopodobieństwo bardzo wysokie, jeśli ryzyko występuje często, średnio co rok
5.	80–100%	Krytyczne	Prawdopodobieństwo krytyczne, jeśli ryzyko występuje częściej niż raz na rok

Źródło: na podstawie opracowania: E.I. Szczepankiewicz, *Wykorzystanie punktowej metody oszacowania ryzyka operacyjnego w instytucjach finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 298.

[244] J.K. Solarz, *Zarządzanie ryzykiem systemu finansowego*, Warszawa 2005.
[245] E.I. Szczepankiewicz, *op. cit.*

Tabela 6. Przykładowa interpretacja trzy stopniowej macierzy ryzyka.

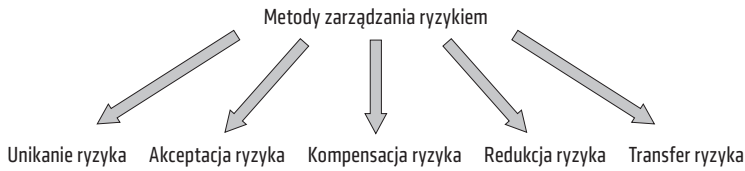
Wysoka częstotliwość	Ryzyko bardzo często występujące i powodujące względnie niskie straty	Ryzyko bardzo często występujące i powodujące dość wysokie straty	Ryzyko krytyczne, występujące z dużą częstotliwością i powodujące wysokie straty – zagraża osiągnięciu celów
Średnia częstotliwość	Ryzyko dość systematycznie występujące i powodujące niskie straty	Ryzyko dość systematycznie występujące i powodujące dość wysokie straty	Ryzyko dość systematycznie występujące i powodujące wysokie straty
Niska częstotliwość	Ryzyko rzadko występujące i powodujące niskie straty	Ryzyko rzadko występujące, ale powodujące dość wysokie straty	Ryzyko rzadko występujące, ale powodujące wysokie straty
	Niskie straty	**Średnie straty**	**Wysokie straty**

Oszacowanie ryzyka daje podstawę do podejmowania decyzji o postępowaniu z ryzykiem oraz stanowi podstawę projektowania odpowiednich procedur kontrolnych. Ma to podstawowe znaczenie dla skutecznego i efektywnego zarządzania działalnością instytucji. Przyjmując dwa omawiane kryteria oceny ryzyka, można wskazać zasadnicze typy zarządzania ryzykiem. W wypadku działań o niskim stopniu ryzyka podejmuje się na ogół decyzję o jego akceptacji oraz niepodejmowaniu działań interwencyjnych. Dopiero średni poziom ryzyka (czy to prawdopodobieństwa jego wystąpienia, czy to dolegliwości skutków jego ziszczenia się) wymaga ciągłego monitorowania oraz podjęcia działań mających na celu redukcję prawdopodobieństwa ryzyka i dolegliwości jego skutków. W przypadku wysokiego ryzyka zasadne jest natomiast, oprócz zastosowania wymienionych już sposobów zarządzania ryzykiem, ubezpieczenie się na wypadek wystąpienia negatywnych skutków przewidywanego zdarzenia. W ekstremalnych przypadkach, gdy ryzyko jest nieproporcjonalnie wysokie w stosunku do ewentualnych zysków, należy podjąć decyzję o rezygnacji z procesu, w związku z którym ono występuje[246].

Jak już wspomniano, dopiero prawidłowa identyfikacja ryzyka pozwala wdrożyć odpowiednie procedury jego ograniczenia. Wskazać należy siedem głównych sposobów zarządzania ryzykiem przez instytucje finansowe, co obrazuje poniższy rysunek.

[246] R. Kendall, *Zarządzanie ryzykiem dla menedżerów. Praktyczne podejście do kontrolowania ryzyka*, Warszawa 2000.

Rysunek 3. Metody zarządzania ryzykiem.



Źródło: opracowanie własne na podstawie E. Dziawgo, *Zarządzanie ryzykiem rynkowym w przedsiębiorstwie w warunkach kryzysu zaufania Ewa Dziawgo,* http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ekon-element-000171224075 [dostęp: 31.05.2019].

Przez unikanie ryzyka rozumie się na ogół całkowite powstrzymanie się od działań i udziału w procesach, z którymi wiąże się dane ryzyko. Wskazać należy, że nie każdy rodzaj ryzyka można ograniczyć w ten sposób – wynika to zarówno z charakteru danego ryzyka, jak i z potrzeby realizowania nadrzędnego celu każdego podmiotu działającego na rynku finansowym, tj. osiągnięcia zysku. Akceptacja ryzyka przejawia się w znoszeniu przez dany podmiot ewentualnych negatywnych skutków jego ziszczenia się. Zarządzanie ryzykiem w powyższy sposób sprowadza się do określenia poziomu ryzyka, od którego poprzestawanie jedynie na jego tolerowaniu staje się niedopuszczalne. Na ogół chodzi o wskazanie sytuacji, w których szeroko rozumiane straty podmiotu okazują się na tyle dolegliwe, iż podjęcie działań zmierzających do ich ograniczenia staje się rozwiązaniem tańszym niż dalsza akceptacja ryzyka. Kompensata ryzyka jako sposób zarządzania nim sprowadza się natomiast do takiego ukształtowania struktury działalności, które pozwoli na pokrywanie strat powstałych w związku z danym ryzykiem przez zyski pochodzące z innych niezwiązanych z nim operacji. Redukcja ryzyka rozumiana jest natomiast jako podejmowanie działań zaradczych, mających ograniczać zarówno prawdopodobieństwo ryzyka, jak i dolegliwość negatywnych skutków jego urzeczywistnienia się. Przykładem działań mających na celu właśnie redukcję ryzyka będzie np. zachowanie ostrożności w doborze partnerów biznesowych oraz stosowanie odpowiednich klauzul umownych. Ostatnim z wyróżnionych sposobów zarządzania ryzykiem jest

transfer ryzyka. Polega on na zobowiązaniu innego podmiotu do ponoszenia negatywnych skutków ziszczenia się ryzyka np. poprzez ubezpieczanie się[247].

Transfer ryzyka jest jednym z najważniejszych sposobów zarządzania nim. Niewątpliwie na jego popularność ma wpływ fakt, że ze względu na elastyczność umów ubezpieczenia możliwe jest przetransferowanie praktycznie każdego rodzaju ryzyka. Należy jednak zaznaczyć, że celem tej konkretnej metody zarządzania ryzykiem nie jest ograniczenie prawdopodobieństwa urzeczywistnienia się ryzyka – transfer pozwala jedynie na zmniejszenie dolegliwości ewentualnych skutków danego ryzyka. Transfer ryzyka dokonywany jest m.in. w drodze przyjęcia przez inny podmiot odpowiedzialności za ewentualne straty w drodze umowy ubezpieczenia lub zastosowanie klauzul umownych wyłączających odpowiedzialność za straty wynikłe przy realizacji kontraktu. Kolejnym sposobem dokonywania transferu ryzyka jest transfer działalności wiążącej się z tym ryzykiem – inny podmiot wykonuje daną działalność, przez co naraża się na wspomniane negatywne skutki. Ostatnim ze sposobów transferu ryzyka jest *hedging*, czyli korzystanie z instrumentów pochodnych celem ograniczania ryzyka[248].

Stosowanie działań interwencyjnych i aktywne ograniczanie ryzyka wymaga stałego analizowania jego poziomu. Pozwala to wykryć wypadki, w których ryzyko w wyniku zmiany okoliczności przestaje być minimalizowane przez stosowane do tej pory działania oraz dokonać stosownej korekty obranej strategii.

5.6. Ryzyko przestępczości finansowej

W literaturze przedmiotu pojęcie „przestępczości finansowej" obejmuje najczęściej swym zakresem przestępstwa w sektorze finansowym i kapitałowym, a także przestępczość ubezpieczeniową, przestępstwa celne i podatkowe oraz przestępstwa piractwa intelektualnego i przemysłowego. Sformułowanie szczegółowej definicji przestępczości finansowej jest zadaniem niezwykle

[247] W. Tarczyński, M. Mojsiewicz, *Zarządzanie ryzykiem. Podstawowe zagadnienia*, Warszawa 2001.

[248] P. Matkowski, *op. cit.*

trudnym z uwagi na fakt, iż jest to określenie niezwykle szerokie. Możliwe jest natomiast wskazanie cech charakterystycznych przestępstw przeciw interesom instytucji finansowych. Są to brak przemocy w *modus operandi*, wysokie zyski, anonimowość ofiar, specyfika sprawców tych czynów (często są to członkowie zorganizowanych grup przestępczych)[249].

Podkreślenia wymaga fakt, że to właśnie instytucje finansowe, w szczególności banki, ze względu na mnogość dokonywanych operacji oraz ich wartość są szczególnie narażone na ryzyko przestępczości.

Analiza relacji pomiędzy przestępczością zorganizowaną a sektorem bankowym pozwala na wskazanie konkretnych płaszczyzn, na których dochodzi do ich zetknięcia się[250].

Płaszczyznę pierwszą sprowadzić można do tzw. przestępstw zewnętrznych. Należy zauważyć, że przestępcy traktują banki jako nieograniczone źródło środków pieniężnych. Poszczególne grupy przestępcze różnią się przyjętymi metodami wyprowadzania pieniędzy poza system finansowy w zależności od swego charakteru oraz zdolności. Nie będzie zaskoczeniem stwierdzenie, że grupy kryminalne będą się ograniczać głównie do przemocy, celem wejścia w posiadanie środków finansowych, natomiast grupa dysponująca zasobami intelektualnymi skupi się raczej na dokonywaniu wyrafinowanych oszustw lub wyłudzeń.

Druga płaszczyzna polega na współdziałaniu podmiotów należących do struktury organizacyjnej instytucji finansowej z przestępcami, co określa się mianem oszustwa wewnętrznego. Celem takiej współpracy jest wykorzystanie wiedzy pracownika banku na temat przyjętych metod zarządzania ryzykiem dla zdobycia środków finansowych.

Trzecia płaszczyzna polega na korzystaniu z wiedzy posiadanej przez instytucje bankowe na szkodę osób trzecich, czyli na zdobywaniu przez przestępców danych wrażliwych klientów banków.

Poczynione rozważania prowadzą do wniosku, że do wzrostu ryzyka operacyjnego, ściślej ryzyka przestępstw finansowych, przyczyniają się wadliwe procedury bezpieczeństwa obowiązujące w danej instytucji finansowej lub sami pracownicy danej instytucji, którzy łamią prawidłowe, w teorii znacznie

[249] J. Koleśnik, *Bezpieczeństwo systemu bankowego. Teoria i praktyka*, Warszawa 2011.
[250] A. Buszko, *Finanse przestępczości zorganizowanej*, Toruń 2014.

ograniczające niebezpieczeństwo, poprawne metody zarządzania ryzykiem operacyjnym. Oszustwa za to mogą godzić w interesy instytucji finansowej (tu wymienić należy wyłudzenia wsparcia finansowego), jej klientów (kradzież danych oraz środków finansowych przekazanych instytucji) albo też całego rynku finansowego (zasadniczo pranie brudnych pieniędzy).

Na uwagę zasługuje również charakter wielu przestępstw finansowych – sytuacyjny, okazjonalny. Przestępcy finansowi korzystają z luk w procedurach i zabezpieczeniach stosowanych przez instytucje finansowe. Podobnie pracownicy instytucji finansowych angażują się w działalność przestępczą dopiero po nabraniu przekonania, iż nie dojdzie do wykrycia wywołanych przez nich nieprawidłowości w systemie danej instytucji. Warto zatem wskazać, iż jakość reguł zarządzania ryzykiem w danej instytucji ma charakter decydujący dla ograniczenia ryzyka związanego z przestępczością finansową.

5.7. Podsumowanie – postulaty *de lege ferenda*

Podkreślić należy, iż z uwagi na mnogość rodzajów instytucji finansowych oraz różnorodność dokonywanych przez nie operacji nie jest możliwe wskazanie jednego szczegółowego wzoru zarządzania ryzykiem operacyjnym skutecznie ograniczającego ryzyko dla każdej instytucji finansowej. Konkretne reguły postępowania winny zostać opracowane przez odpowiednie organy samej instytucji finansowej tak, by były dostosowane do specyfiki prowadzonej działalności oraz indywidualnych uwarunkowań podmiotu[251]. Nie ulega jednak wątpliwości, iż możliwe jest sformułowanie szeregu wytycznych, zgodnie z którymi instytucje powinny przygotować wewnętrzne zasady zarządzania ryzykiem.

Zauważyć należy, że nie jest możliwe wskazanie jednego systemu, który w sposób całkowity eliminowałby ryzyko związane z operacjami finansowymi. Ryzyko stanowi nieodłączną część działalności gospodarczej. Nie wydaje się również możliwe precyzyjne matematyczne określenie stopnia występującego ryzyka. Stosowane powszechnie metody pozwalają jedynie

[251] J. Zawiła-Niedźwiecki, *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, Kraków 2013.

na określenie prawdopodobieństwa pewnych zdarzeń w sposób subiektywny i intuicyjny, oparty na posiadanym doświadczeniu życiowym. Wiążą się z tym również problemy z dokładnością oceny relewantności określonych zagrożeń oraz czynniki związane ze społecznymi oczekiwaniami na temat poziomu bezpieczeństwa publicznego.

Omawiane zjawiska nie ograniczają się wyłącznie do kwestii bezpieczeństwa instytucji finansowych. Ryzyko występuje przy każdym rodzaju działań podejmowanych w rzeczywistości rynkowej. Również pewne elementy związane z procedurami zarządzania ryzykiem wydają się wspólne dla większości sytuacji, jak np. pewna uciążliwość procedur bezpieczeństwa dla personelu oraz związane z tym wydłużenie czasu trwania procedur. Powszechne wydaje się zjawisko interpretowania przez pracowników norm systemu bezpieczeństwa jako skierowanych przeciw nim. Wydaje się, że opinia ta jest uzasadniona z uwagi na fakt, że – jak już wskazywano – większość strat ponoszona jest przez instytucje z powodu zaniedbań lub celowych działań pracowników. Wydaje się, że opracowując metody radzenia sobie z ryzykiem, konieczne jest takie określenie procedur ochronnych, aby surowość systemu pozostawała w zgodzie ze zdrowym rozsądkiem oraz równowaga z wytrzymałością i kondycją pracowników[252]. Zbyt duża surowość procedur prowadzić może personel do wniosku, że władze przedsiębiorstwa traktują ich jako element potencjalnie wrogi i obcy, co może skutkować zwiększeniem się poziomu ryzyka.

Niniejsza analiza pozwala jednak niewątpliwie na sformułowanie kilku postulatów, których przestrzeganie przez instytucje finansowe powinno znacząco obniżyć poziom ryzyka operacyjnego, na jakie narażone.

Propozycje praktyk służących ograniczeniu ryzyka operacyjnego

Wydaje się, iż konieczne jest szczegółowe rozplanowanie procesu zarządzania ryzykiem operacyjnym w każdej instytucji finansowej. Dobry plan zarządzania ryzykiem powinien się składać z 6 elementów: identyfikacja ryzyka, ocena ryzyka, monitorowanie ryzyka, raportowanie ryzyka, kontrola ryzyka, działania zabezpieczające.

[252] E. Skrzypek, *Zarządzanie ryzykiem i zmianami w organizacji*, Lublin 2015.

Zaproponowany model zarządzania ryzykiem zdaje się w najpełniejszy sposób spełniać potrzeby związane z ograniczeniem ryzyka operacyjnego. Wdrożenie omawianego modelu, wraz z jednoczesnym dostosowaniem do potrzeb konkretnych przypadków oraz charakteru danej instytucji finansowej, wydaje się korzystne w kontekście poprawy bezpieczeństwa danej instytucji. Procedury identyfikowania ryzyka obowiązujące w danej instytucji prowadzić powinny do podejmowania trafnych i skutecznych decyzji w oparciu o możliwie pełny zestaw danych. Szczególnie starannej kontroli podlegać powinny działania pracowników instytucji oraz stan wykonania zadań przez samą instytucję w ramach osiąganych przez nią celów.

Najskuteczniejszym, choć często niedocenianym, sposobem ograniczania ryzyka operacyjnego w instytucji jest stworzenie etycznego środowiska pracy. Brak odpowiednich standardów etycznych zinternalizowanych przez personel instytucji jest jednym z głównych czynników odpowiedzialnych za oszustwa wewnętrzne. Pracownicy niepoczuwający się do lojalności w stosunku do pracodawcy są bardziej skłonni do ugięcia się pod presją i dokonania oszustwa lub do ignorowania niepokojących zdarzeń. Wykształcenie standardów etycznych w instytucji finansowej wymaga kompleksowych działań – przede wszystkim konieczne jest przygotowanie jasnych zasad postępowania personelu w określonych sytuacjach. Rozwiązanie to pozwala ograniczyć niepewność popychającą pracowników do przemilczania ewentualnych nieprawidłowości. Równie konieczne wydaje się opracowanie kanałów komunikacyjnych umożliwiających członkom personelu pozyskiwanie infomacji na temat porządanych przez kierownictwo instytucji wzorców zachowań w sytuacjach nowych bądź kontrowersyjnych. Kolejnym elementem podnoszenia standardów etycznych w instytucji wydaje się podjęcie działań mających na celu wzbudzenie poczucia lojalności pracowników w stosunku pracodawcy – jako przykład wskazać tu należy programy wsparcia dla pracowników. Jedną z przesłanek wpływających na ryzyko oszustwa jest odczuwanie przez pracowników presji – efektywnym rozwiązaniem będzie zatem eliminacja lub ograniczenie odczuwanej przez personel presji finansowej. Właśnie jej ograniczeniu służy wprowadzenie programów pomocowych – szkoleń podnoszących kwalifikacje czy pracowniczych ubezpieczeń zdrowotnych. Etyczne środowisko pracy sprawi, że pracownicy rzadziej będą

decydować się na działalność na szkodę instytucji oraz częściej będą zgłaszać dostrzeżone nieprawidłowości.

Niezwykle ważnym elementem w kontekście bezpieczeństwa instytucji jest również zdolność kadry zarządzającej do ponoszenia ryzyka oraz prawidłowego zarządzania nim, poprzez prawidłową ocenę charakteru ryzyka, ewentualnego rachunku zysków i strat oraz szeregu czynników wewnętrznych i zewnętrznych. Wymaga to stałego podnoszenia kwalifikacji kadry kierowniczej oraz podziału kompetencji ograniczającego konflikt interesów.

Szczególnemu badaniu powinny więc podlegać takie elementy: zasady etyczne, cele i zadania przypisane konkretnym pracownikom, delegowanie uprawnień i odpowiedzialności czy dzielenie się wiedzą. Zachowanie odpowiedniej kultury i etosu pracy wśród pracowników powinno prowadzić do minimalizacji części ryzyka związanego z prowadzoną działalnością.

Do najważniejszych zadań zarządu danej instytucji zaliczyć należy sformułowanie strategii zarządzania ryzykiem operacyjnym oraz określenie konkretnych i szczegółowych procedur i wytycznych realizacji zarządzania ryzykiem. Prawidłowo opracowana strategia, zawierająca w sobie takie elementy, jak: definicja ryzyka operacyjnego, profil ryzyka instytucji, skala i struktura ryzyka, procedury zarządzania ryzykiem, system kontroli wewnętrznej, powinna podlegać zatwierdzeniu oraz bieżącej weryfikacji przez odpowiednie ograny konkretnego podmiotu, jak np. rada nadzorcza itp., działania te pozwalają opracować właściwy dla danej instytucji model zarządzania pozwalający na zachowanie ładu korporacyjnego[253].

Skuteczność zarządzania ryzykiem operacyjnym wymaga jasnego podziału kompetencji oraz struktury organizacyjnej i podległościowej w danej instytucji w zakresie zarządzania ryzykiem. Odpowiedzialność związana z zarządzaniem ryzykiem na danym szczeblu organizacyjnym spoczywa na kierownictwu danego szczebla. Warunkiem prawidłowości zachodzących procesów jest znajomość zasad i strategii zarządzania ryzykiem operacyjnym przez kadrę menedżerską. Konieczne wydaje się stworzenie w strukturze organizacyjnej jednostki stanowiska lub zespołu odpowiedzialnego za zarządzanie poszczególnymi rodzajami ryzyka, zwłaszcza ryzyka oszustw oraz zapewnienie jego niezależności. Jasne określenie podmiotu odpowiedzialnego

[253] M. Capiga, J. Harasimowicz, G. Szustak, *Finanse banków*...

w razie wystąpienia nieprawidłowości wpłynie niewątpliwie pozytywnie na jakość zarządzania. Dla skuteczności podejmowanych działań niezwykle ważne jest również, aby istniał system kanałów informacyjnych umożliwiających komunikację pomiędzy zarządem a podmiotami odpowiedzialnymi za bieżące zarządzanie ryzykiem. Dzięki temu możliwe jest sprawne działanie systemu bezpieczeństwa danej instytucji.

Wydaje się również, że nieodzownym warunkiem skuteczności podejmowanych działań jest istnienie w strukturze danej instytucji ciała odpowiedzialnego za audyt wewnętrzny, posiadającego odpowiednie kwalifikacje oraz możliwości bieżącej oceny stanu działalności danej instytucji. Efektem audytu powinny być raporty przedstawiane kierownictwu na temat efektywności prowadzonych działań w związku z występującym ryzykiem. Nie można jednak odpowiedzialności za zarządzanie ryzykiem, ciążącej na zarządzie, przerzucać na komórkę audytu wewnętrznego.

Z uwagi na specyfikę działalności w sferze gospodarczej wszelkie procedury i strategie zarządu ryzykiem powinny być nieustannie analizowane i dostosowywane do zmieniających się okoliczności rynkowych przez kierownictwo danej instytucji.

Podsumowując, wskazać należy, że konieczne jest jasne określenie podmiotów odpowiedzialnych za zarządzanie ryzykiem operacyjnym oraz zapewnienie im niezależności. Równie ważne jest takie ukształtowanie struktury organizacyjnej instytucji, by jednostki te nie pozostawały w konflikcie interesów w związku z przydzielonymi im zadaniami. Powinny one również pozostawać w nieustannej świadomości procesów zachodzących w ramach ryzyka związanego z prowadzoną działalnością oraz nieustannie dostosowywać swe działania do zmieniających się okoliczności, w celu podejmowania prawidłowych decyzji w ramach zarządzania ryzykiem.

W polskim porządku prawnym można znaleźć kluczowy przepis ustawy mówiący o obowiązku skonstruowania w instytucji finansowej systemu zarządzania ryzykiem, który dotyczy nie tylko instytucji finansowych, ale też ich podmiotów zależnych[254]. Art. 9 ust. 3 pkt 1 pr. bank.[255] konstytuuje

[254] G. Sikorski, *Prawo Bankowe. Komentarz*, Warszawa 2015, Art. 9b, Nb 2.

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

taki obowiązek, którego szczegóły określone są przez kolejne przepisy tej ustawy. I tak art. 9b dostarcza definicji zadań systemu zarządzania ryzykiem. Ustawodawca zakwalifikował do nich *identyfikację, pomiar lub szacowanie, kontrolę oraz monitorowanie ryzyka występującego w działalności banku służące zapewnieniu prawidłowości procesu wyznaczania i realizacji szczegółowych celów prowadzonej przez bank działalności*. W dalszej części zostały też określone instrumenty, które powinny być używane w ramach systemu zarządzania ryzykiem. Prawodawca zakwalifikował do nich:

1) sformalizowane zasady służące określaniu wielkości podejmowanego ryzyka i zasady zarządzania ryzykiem;
2) sformalizowane procedury mające na celu identyfikację, pomiar lub szacowanie oraz monitorowanie ryzyka występującego w działalności banku, uwzględniające również przewidywany poziom ryzyka w przyszłości;
3) sformalizowane limity ograniczające ryzyko i zasady postępowania w razie przekroczenia limitów;
4) system sprawozdawczości zarządczej służący monitorowaniu poziomu ryzyka;
5) strukturę organizacyjną adekwatną do wielkości i profilu ponoszonego przez bank ryzyka.

Komplementarny dla tego aktu prawnego jest szereg doprecyzowujących unormowań dotyczących systemu zarządzania ryzykiem, który znajduje się w rozporządzeniu Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach[256]. W tym akcie jednak, podobnie jak w ustawie, trudno znaleźć szczegółowe przepisy odnoszące się do zarządzania ryzykiem w kontekście przeciwdziałania przestępczości. Jedynym odniesieniem jest regulacja zgłaszania nieprawidłowości wewnątrz instytucji finansowych (sygnalizm). Pozostałe instrumenty wiążą się z gospodarczymi standardami wymaganymi od instytucji finansowych.

[256] Rozporządzenie Ministra Rozwoju i Finansów z dnia 6 marca 2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (Dz.U. 2017 r., poz. 637).

Przechodząc do części postulatywnej opracowania, należy stwierdzić, że regulacje dotyczące zarządzania ryzykiem mają szczególny charakter. Przepisy te są raczej domeną wewnętrznych decyzji jednostek organizacyjnych, gdyż jest to podyktowane złożonością prowadzonej działalności gospodarczej. Na poziomie ustawodawcy przepisy mogą mieć charakter raczej ogólnych kierunków niż gotowej struktury organizacyjnej, która pozwoli ograniczyć przestępczość w instytucjach finansowych.

Zarządzanie Ryzykiem Przestępczości (CRM) jest ewolucyjnym i analitycznym procesem mającym na celu:

- ocenę, czy procedury organizacyjne, aktywa lub osoby fizyczne mogą być narażone na potencjalne zagrożenie;
- określenie środków niezbędnych do zmniejszenia takiego ryzyka;
- złagodzenie konsekwencji jakiegokolwiek zagrożenia po jego wystąpieniu;
- ocenę powodzenia lub innych zalecanych działań oraz ich odpowiednie dostosowanie.

Konwencje zarządzania ryzykiem uwzględniają fakt, że chociaż jest mało prawdopodobne, aby ryzyko zostało całkowicie wyeliminowane, dostosowanie organizacyjnych mechanizmów bezpieczeństwa w celu dalszej ochrony przed przewidywanymi lub wyobrażonymi zagrożeniami może je znacznie ograniczyć.

Proces zarządzania ryzykiem kryminalnym zapewnia osobom odpowiedzialnym za zabezpieczenie organizacji przed ryzykiem różne narzędzia. Gdy stosowane są najlepsze praktyki, proces CRM może również mieć efekt odstraszający od przyszłych nadużyć, gdy ukryte słabe punkty operacji zostaną rozpoznane i odpowiednio ograniczone do akceptowalnych granic.

CRM można sprowadzić do następujących zadań[257]:

- ocenę ryzyka za pomocą środków proaktywnych, a nie tylko reagowanie na ryzyko w momencie jego wystąpienia,
- ocenę potencjalnych strat, które mogą wynikać z tych ewentualności,
- przeprowadzenie analizy kosztów i korzyści wynikających z podjęcia środków interwencyjnych w zakresie ryzyka,

[257] M. Gill, *Chapter 1. Introduction*, [w:] *Crime at Work Volume II. Increasing the Risk to Offenders*, red. *idem*, Leicester 1998, s. 11–23.

- zminimalizowanie, kontrolę lub przeniesienie przewidywalnego ryzyka.

Dlatego też solidne podejście do zarządzania ryzykiem obejmuje trzy podstawowe elementy: ocenę zagrożenia, ocenę podatności na zagrożenia oraz ocenę krytyczności[258]. Każdy z tych aspektów uwzględnia również prawdopodobieństwo wystąpienia zdarzenia oraz ramy czasowe, w których może ono wystąpić w czasie trwania projektu[259].

Oceny zagrożeń są krytycznym wsparciem przy podejmowaniu decyzji operacyjnych w fazie projektowania programu bezpieczeństwa, identyfikując obszary wymagające kluczowych i skoordynowanych wysiłków. Ponieważ nie ma możliwości przewidzenia każdego możliwego ryzyka lub poznania wszystkiego o każdym ryzyku, dwa pozostałe procesy związane z tą metodą, oceną podatności i krytyczności, są niezbędne do maksymalizacji gotowości na zagrożenie naruszeniem. Ocena podatności określa *słabości, które mogą być wykorzystane* przez potencjalnych sprawców i *sugeruje możliwości wyeliminowania lub złagodzenia tych słabości*. *Ocena krytyczności to proces mający na celu systematyczną identyfikację i ocenę*: kluczowe zasoby operacji oparte na ich konsekwencjach dla wypełnienia jej misji lub podstawowej funkcji, zasoby w organizacji, które mogą okazać się wrażliwe[260].

Ten aspekt podejścia CRM jest nieodzowny, ponieważ ma on potencjał, aby wspomóc przygotowanie na zagrożenia materialne, a z kolei zwiększyć alokację ograniczonych zasobów na te obszary, czy to na aktywa, procedury czy struktury, które następnie zostały zidentyfikowane jako obszary o najwyższym priorytecie i tym samym wymagają *szczególnej ochrony* przed postrzeganymi zagrożeniami[261].

Podczas gdy wiele konwencjonalnych teorii jest zarówno dostępnych, jak i możliwych do zastosowania jako procesy CRM, dwie współczesne metody, które są najbardziej popularne, stanowią naturalny wybór. W rutynowym podejściu do działalności uwzględnia się jedynie bezpośrednie zagrożenia, w przypadku których co najmniej jeden sprawca przejmuje lub niszczy

---

[258] R.J. Decker, *Homeland Security. Key Elements of a Risk Management Approach*, United States 2001.

[259] Air Force Material Command Pamphlet. Acquisition. Risk Management, AFMC Pamphlet 63–101, 1997.

[260] *Ibidem.*

[261] *Ibidem.*

mienie co najmniej jednej innej osoby. Opiera się więc na trzech czynnikach: *prawdopodobnych przestępcach, odpowiednich celach i braku kompetentnych strażników, zapobiegających przestępstwom*[262]. Z drugiej strony, racjonalne podejście do wyboru skupia się na zapobieganiu przestępczości sytuacyjnej, przewidywaniu czasu i miejsca, w którym mogą wystąpić przestępstwa, ograniczając możliwości i motywację do popełnienia przestępstwa, a tym samym zmniejszając skłonność przestępcy do popełnienia przestępstwa w ogóle[263]. Oba te podejścia podkreślają znaczenie asymilacji i analizy informacji. W tym celu analiza modelu przestępstwa i przestępczości jest krytycznym narzędziem informacyjnym.

Wstępne rozważania nad tymi koncepcjami wydają się stosunkowo proste, jednak perspektywa wdrożenia skutecznego procesu CRM w celu odpowiedniego zabezpieczenia się przed ryzykiem może być dla kierownika ds. bezpieczeństwa zniechęcającym przedsięwzięciem. Jednym z obszarów wymagających kompleksowego podejścia CRM jest w szczególności sektor bankowości detalicznej.

W przypadku stosowania procesu CRM do tej przestępczości w instytucjach finansowych pierwszym krokiem, jaki powinien podjąć kierownik ds. bezpieczeństwa, jest faza wstępnej oceny, która obejmuje ocenę zagrożeń i obszarów podatności w celu określenia poziomu ryzyka. Na tym etapie wymagana jest pewna liczba narzędzi, z których jedne mają charakter ilościowy, a inne jakościowy[264].

W celu określenia nadzwyczajnych zachowań instytucje finansowe zazwyczaj śledzą historię transakcji swoich klientów. Dotyczy to w szczególności instytucji, które wydają karty kredytowe na zakupy kredytowe, a kluczowe znaczenie ma przeglądanie inwestycji w profilowaniu bazy danych historii transakcji z klientami. Systemy te umożliwiają scharakteryzowanie potencjalnych „podejrzanych" incydentów poprzez zaprogramowanie wzorców programowych, które uruchamiają ostrzeżenia, w tym: nagłe spadki wydatków, osiągnięcie limitu kredytowego lub wyczerpanie salda konta, duplikaty

[262] L.E. Cohen, M. Felson, *Social Change and Crime Rate Trends*, „American Sociological Review" 1979, vol. 44.

[263] R.V. Clarke, D.B. Cornish, *Modelling Offenders Decisions. A Framework for Research and Policy*, „Crime and Justice" 1985, vol. 6.

[264] L.J. Fennelly, *Handbook of Loss Prevention and Crime Prevention*, Amsterdam 2003.

transakcji mało prawdopodobnych towarów, szczególnie drogich. Przykładem zautomatyzowanego programowania wykorzystywanego do wykrywania nietypowych aktywności na rachunkach kart jest funkcja inteligentnego punktowania ryzyka (VISOR) oferowana przez sieć Visa[265]. Zastosowanie tej techniki poprawiło potencjał zmniejszenia wpływu oszustw zarówno na klientów, jak i instytucje, jednocześnie zapobiegając dalszym kradzieżom i działając jako środek odstraszający aspirujących przestępców. Oceny jakościowe określają szanse na ryzyko w skali od znikomej do zaporowej w oparciu o opinie, doświadczenie i wiedzę wiodących ekspertów w dziedzinie zarządzania bezpieczeństwem[266]. Biorąc pod uwagę, że większość oszustw związanych z płatnościami ma miejsce w punktach sprzedaży, a ponieważ wysoko wykwalifikowani menedżerowie ds. bezpieczeństwa nie mogą monitorować wszystkiego na raz, jednym z najskuteczniejszych sposobów włączenia oceny jakościowej do procesu CRM jest wdrożenie kompleksowego systemu szkoleń dla pracowników wraz z szeroko zakrojoną kampanią uświadamiającą, mającą na celu edukowanie klientów i instalowanie sprzętu do stałego nadzoru, takiego jak telewizja przemysłowa[267]. To podwójne podejście instruuje na temat różnych metod stosowanych w celu niewłaściwego wykorzystania kart lub informacji o kartach w celu stworzenia mechanizmu obrony przed linią frontu i zwiększenia zdolności wykrywania oszustw w ramach operacji. Wszelkie działania przestępcze przechwycone przez personel są szybko komunikowane w całej organizacji, w celach instruktażowych i dochodzeniowych oraz w celu dalszego wspierania tej samoregulacyjnej metody[268].

W wyniku asymilacji ilościowej i jakościowej analizy do najlepszych praktyk w sektorze bankowym CRM zaowocowało wprowadzeniem szeregu skutecznych kontroli zaprojektowanych specjalnie w celu ograniczenia oszustw. Jednym z rozwiązań było wprowadzenie w Wielkiej Brytanii wbudowanego zabezpieczenia mikroprocesorowego i kart PIN[269]. Takie

---

[265] P.N. Grabosky, R.G. Smith, *Crime in the Digital Age. Controlling Telecommunications and Cyberspace Illegalities*, „Transaction Publishers" 1998, no. 1, s. 170.

[266] G.L. Kovacich, W.C. Boni, *High Technology Crime Investigator's Handbook*, Boston 2000, s. 192.

[267] D.J. Horan, *The Retailer's Guide to Loss Prevention and Security*, Floryda 1996, s. 68–76.

[268] *Ibidem*, s. 68.

[269] J. Hoare, *Deceptive Evidence. Challenges in Measuring Fraud*, [w:] *Surveying Crime in the 21st Century*, red. J.M. Hough, M.G. Maxfield, Cullompton 2007, s. 274.

zwiększenie bezpieczeństwa zapobiega niewłaściwemu wykorzystaniu kart kredytowych poprzez żądanie kodu PIN karty przy każdej transakcji, niezależnie od tego, czy klient dokonuje prostego zakupu czy wypłaty gotówki, co jeszcze bardziej zmniejsza ryzyko nieuczciwych transakcji. Takie podejście jest następnie łączone z doradztwem dla klientów, jak konieczność oddzielnego przechowywania kart i informacji PIN[270]. Przy wdrażaniu tego rodzaju systemów zarządzania ryzykiem związanym z przestępczością należy jednak pamiętać o dwóch nadrzędnych względach, którymi powinni kierować się menedżerowie ds. bezpieczeństwa, opowiadając się za daną metodą: prawdopodobieństwie oraz związanych z tym wynikach w zakresie kosztów i korzyści.

Zwolennicy zarządzania przestępczością zalecają, aby ryzyko było zawsze postrzegane w kontekście probabilistycznym[271]. Na przykład niedawny upadek rynku kredytów hipotecznych typu *sub-prime*, który rozpoczął się w Stanach Zjednoczonych, wywarł ogromny wpływ na światowe rynki finansowe, jednak organizacje, które postrzegały prawdopodobieństwo wystąpienia tego zdarzenia jako możliwe, zdalnie zainstalowały mniej środków mających na celu ubezpieczenie od takiego ryzyka, tym samym ponosząc największe straty. Ten przykład stanowi dowód na to, że obserwatorzy, którzy postrzegali tę praktykę jako wątpliwą, choć nie przestępczą w najściślejszym tego słowa znaczeniu, i którzy nadal opowiadali się za bardziej rygorystycznymi regulacjami w zakresie udzielania kredytów[272].

Drugim, i prawdopodobnie ważniejszym, czynnikiem jest fakt, że koszt wdrożenia CRM nie powinien przekraczać korzyści uzyskanych przez instytucję w celu uniknięcia ryzyka[273]. Powszechność oszustw, choć przynosząca straty, nie spowoduje, że zostaną zainstalowane zaawansowane systemy zarządzania ryzykiem we wszystkich miejscach sprzedaży. Jedna z bardziej dramatycznych ostatnich propozycji przeciwdziałania przestępstwom o charakterze oszustwa tożsamości polega na biometrycznym oznaczaniu osób za pomocą odpowiedniego dowodu tożsamości w celu opracowania rejestru wszystkich działań, który jest następnie kompilowany do centralnej

[270] P.N. Grabosky, R.G. Smith, *op. cit.*, s. 170.

[271] R.J. Fischer, G. Green, *Introduction to Security (7th Edn)*, Amsterdam 2004, s. 139.

[272] M. Munro, J. Ford, C. Leishman, N.K. Karley, *Lending to Higher Risk Borrowers. Sub-prime Credit and Sustainable Home Ownership*, The Homestead 2005.

[273] C.L. Culp, *The Risk Management Process*, New Jersey 2001, s. 226.

bazy danych[274]. Chociaż niektórzy uważają te środki za jedyny możliwy sposób kompleksowego monitorowania i kontrolowania takich przestępstw, z pewnością krytykuje się tę sugerowaną metodę, z uwagi m.in. na zaporowy koszt wdrożenia i utrzymania systemu zdolnego do świadczenia tej usługi, możliwość naruszenia bezpieczeństwa w systemie przechowywania danych osobowych obywateli oraz związane z tym naruszenia swobód obywatelskich i praw człowieka, które mogą zostać podniesione w opozycji do wniosku[275]. W związku z tym analiza kosztów i korzyści oparta na analizie branżowej jest istotnym elementem odpowiedniego projektu CRM.

Wdrożenie procesu CRM w organizacji, niezależnie od środowiska, w którym jest on stosowany, zarówno w sferze publicznej, jak i prywatnej, niesie ze sobą wiele korzyści, dlatego też podejście to w praktyce stale rośnie[276]. To właśnie proaktywny charakter podejścia przyjętego w CRM, pozwalającego na łagodzenie i zapobieganie potencjalnie katastrofalnym skutkom, wyjaśnia, dlaczego jest ono tak dobrze oceniane. Sektor bankowy nie jest sam w sobie podatny na straty z powodu nieuczciwych praktyk; według obliczeń opublikowanych przez brytyjski Home Office Identity Fraud Steering Committee (IFSC) szacuje się, że oszustwa związane z tożsamością stanowią roczny koszt dla gospodarki brytyjskiej w wysokości 1,7 mld GBP[277].

Znaczenie zagrożenia przestępczością jest częściowym czynnikiem motywującym sektor usług finansowych do przyjęcia ogólnobranżowego podejścia do wspólnych praktyk regulacyjnych CRM. System Unikania Nadużyć w Branży Kredytowej (*Credit Industry Fraud Avoidance System* – CIFAS) jest reprezentatywny dla tego trendu i służy współpracy z instytucjami w całym sektorze finansowym i w ogólnym interesie systemu bankowego. Te systemy współpracy są następnie powiązane z szerszą infrastrukturą zarządzania bezpieczeństwem publicznym i dzięki prowadzonym konsultacjom oraz wymianie danych analitycznych nawiązano złożone relacje w celu zwalczania

---

[274] H. von. Ahlefeld, J. Gaston, *Lessons in Danger*, OECD Online Bookshop 2005, s. 79.

[275] I. Grant, *Wave of Criticism Hits Government ID Card Relaunch in ComputerWeekly.com* http://www.computerweekly.com/Articles/2008/03/07/229773/wave-of-criticism-hits-government-id-card-relaunch.htm [dostęp: 23.05.2019].

[276] E. McLaughlin, J. Muncie, *The Sage Dictionary of Criminology*, London 2006, s. 363–364.

[277] Home Office, *Identity Fraud puts £1.7bn Hole in Britain's Pocket*, „Press Releases", 2 February 2006.

przestępstw. Opisywany poziom współpracy został sformalizowany w Zjednoczonym Królestwie poprzez zgodę królewską na ustawę o poważnych przestępstwach z 2007 r. w sprawie zapobiegania nadużyciom finansowym, która pozwala na wymianę informacji z organizacjami zajmującymi się zwalczaniem nadużyć finansowych. W ten sposób podejście CRM poszczególnych instytucji formuje standardy branżowe dla krajowych działaniach policyjnych, a wszystkie współpracują w ramach zaawansowanej sieci poświęconej zarządzaniu przestępczością.

Takie wspólne podejście sektora bankowego do procesów CRM rodzi wielopoziomowe skutki. Wspólna sieć CRM umożliwia uczestnikom dostęp do mechanizmu ciągłej oceny ryzyka, pozwalając całej branży na utrzymanie zbiorowej puli wiedzy ułatwiającej ocenę potencjalnych zagrożeń związanych z konkretnym działaniem, czy to nieprzewidzianych wcześniej, czy też stanowiących część nowej inicjatywy danej instytucji, tworząc bezprecedensowy poziom podziału kosztów i korzyści oraz ilustrując potencjał powszechnego wdrażania najlepszych praktyk (CIFAS, 2007 i FSA, 2008). Organy regulacyjne, takie jak Urząd Nadzoru Usług Finansowych (FSA), posiadający uprawnienia statutowe na mocy ustawy o usługach i rynkach finansowych z 2000 r. (Office of PSI, 2000: Part 1, section 1), zapewniają branży pewną formę ochrony zarówno przed wewnętrznymi, jak i zewnętrznymi oszustwami, poprzez monitorowanie, ocenę i sprawozdawczość praktyk stosowanych w całym sektorze. Organ ten jest organizacją pozarządową finansowaną przez branżę upoważnioną do egzekwowania swoich zaleceń (FSA, 2008). Systemowy poziom zaangażowania, którego przykładem jest podejście sektora bankowego do zarządzania relacjami z klientami w zakresie *plastic fraud* oraz szersze zaangażowanie w zwalczanie oszustw związanych z tożsamością w Zjednoczonym Królestwie, dowodzą wysokiego poziomu współpracy niezbędnej do skutecznego zwalczania konkretnych przestępstw i wykorzystania pełnego potencjału procesów zarządzania relacjami z klientami.

Jak podkreślono powyżej, wysoki poziom współpracy międzysektorowej, niezbędny do rzeczywistego dostrzeżenia i ograniczenia konkretnych przestępstw, często wykracza poza możliwości wywierania wpływu przez osoby zarządzające bezpieczeństwem na małą skalę. Nawet w przypadku ścisłej współpracy sektoru bankowego w celu ograniczenia oszustw, przestępstwa nadal się pojawiają. Jeśli sprawca popełnia pojedyncze przestępstwa, może

istnieć niewielkie ryzyko wykrycia, incydenty mogą nie być rejestrowane lub zgłaszane, a zatem istnieje postrzegany brak kary związanej z przestępstwem, co może zwiększyć powagę problemu (Departament Kryminologii, 2003: 1–21). W miarę jak polityka CRM przesuwa swoją uwagę w kierunku większego obszaru ryzyka, pozostawia się lukę dla niewykrytych sprawców na małą skalę, którzy mimo to przyczyniają się do obszaru działalności oszukańczej, niosącej poważne straty dla kredytodawców.

Największym wyzwaniem w przyjmowaniu podejścia procesowego CRM jest zaprojektowanie systemu w oparciu o „realne" zagrożenia i z wystarczającą elastycznością, aby dostosować się do stale zmieniającego się środowiska. Procesy CRM wymagają ciągłego przeglądu, oceny, ponownej oceny i adaptacji, a nawet wtedy nie ma gwarancji, że ryzyko będzie zawsze unikane[278]. Dlatego też wdrożenie procesu CRM wymaga skrupulatnego badania kosztów i korzyści, wiarygodnej i wysokiej jakości informacji, na podstawie których sporządzana jest ocena ryzyka, oraz hurtowego zaangażowania organizacji w celu uzyskania maksymalnej wartości[279]. Jeśli podejście to jest zbyt konserwatywne, istnieje ryzyko, że namacalne możliwości biznesowe mogą być niepotrzebnie pomijane, a jednocześnie nie uwzględniać ryzyka. Wreszcie kierownik ds. bezpieczeństwa musi również kontrolować poziom oczekiwań związanych z przewidywanym poziomem sukcesu, ponieważ jest mało prawdopodobne, aby nawet najbardziej niezawodny system pozostawał niezmiennie skuteczny.

Podsumowując, prawie każda czynność w biznesie wiąże się z elementem ryzyka: zmianą nawyków klientów, pojawieniem się nowych konkurentów, a czynniki pozostające poza sferą kontroli mogą opóźnić realizację projektu. Jednak dogłębna analiza ryzyka i zarządzanie ryzykiem mogą pomóc w podejmowaniu decyzji i zminimalizowaniu potencjalnego zakłócenia, zwłaszcza gdy istnieje wystarczająca równowaga pomiędzy ograniczeniem ryzyka a związanymi z tym kosztami. Rozwój procesów CRM wykorzystujących zdecentralizowane techniki zarządzania ryzykiem w połączeniu ze scentralizowanym podejściem koordynacyjnym staje się akceptowaną najlepszą praktyką, w wyniku czego poszczególne firmy są w stanie najlepiej

[278] M. Gill, *op. cit.*, s. 17.
[279] *Ibidem*, s. 16–17.

dostosować ramy do swoich preferencji i warunków wewnętrznych. Wydaje się zatem, że dyscyplina ta będzie coraz bardziej popularna, czego dowodem jest przewaga jej praktyki w głównym nurcie. Jednak połączenie ciągłej dynamiki zmian stanowi największe wyzwanie dla kierownika ds. bezpieczeństwa w zakresie ograniczania ryzyka.

ROZDZIAŁ SZÓSTY

Analiza przygotowania obrony przed różnymi formami ataków na instytucje finansowe. *Cybercrimes*

Przeciwdziałanie przestępstwom komputerowym stanowi część składową kompleksowego systemu zarządzania ryzykiem[280]. W celu opracowania analizy prawnej bezpieczeństwa cybernetycznego w sektorze finansowym, wdrażania strategii biznesowych, zarządzania zmianą oraz wdrożenia rozwiązań w sektorze finansowym należy rozpocząć od ogólnego wstępu do problemu przestępstw komputerowych. Z uwagi na ich złożoność i tempo rozwoju trudno stworzyć ich uniwersalną definicję. Można je jednak scharakteryzować dwoma cechami. Po pierwsze, nierzadko trudno przypisać pochodzenie działania przestępnego, noszą one zatem znamiona przestępstw anonimowych. Po drugie, często mają one charakter ponadnarodowy, czym sprawiają ogromne problemy, nie tylko organom stanowienia prawa (problem skoordynowanej walki z przestępczością komputerową), ale też organom stosowania prawa (problem skoordynowanej polityki ścigania przestępstw). Do dodatkowych cech tego typu przestępstw, które sprawiają, że przeciwdziałanie im staje się niezwykle trudne, można zaliczyć:

- ograniczenie kosztu popełnienia przestępstwa;
- ogromną skalę działań przestępnych, które wiążą się z małymi szkodami, które zniechęcają potencjalne ofiary do podjęcia działań prawnych;
- szybki rozwój nowych form popełnianych przestępstw.

Jeżeli zaś chodzi o formy przestępstw komputerowych (*cybercrimes*), to można wyróżnić dwa typy. Pierwszy z nich wiąże się z wykorzystaniem

[280] Chartis Research, *Financial Crime Risk Management Systems Oracle Vendor Highlights 2014*, http://www.oracle.com/us/corporate/analystreports/chartis-financial-crime-risk--2541655.pdf [dostęp: 13.05.2019].

nowoczesnych technologii do popełnienia przestępstwa. Przykładem takiej działalności może być podszywanie się pod kogoś czy fałszowanie tekstu, zdjęć czy innych multimediów. Druga forma polega na zorientowaniu się przestępcy na nowoczesne technologie jako obiekt działania przestępnego. Najbardziej oczywistym przykładem tego typu działalności jest hakowanie systemów informatycznych, czyli uzyskiwanie do nich nieautoryzowanego dostępu przy użyciu szkodliwego oprogramowania.

Kluczowym aktem prawnym, powiązanym ze zjawiskiem przestępczości komputerowej, jest *The Cybercrime Convention*[281] (*Budapest Convention*) uchwalona przez Radę Europy w 2001 roku. Zgodnie z elementarnymi postanowieniami Konwencji obligującymi kraje ratyfikujące ją do stworzenia mechanizmów reagowania na przestępstwa komputerowe, te ostatnie można podzielić na:

- przestępstwa przeciwko spójności i dostępowi do danych i systemów komputerowych;
- przestępstwa związane z użyciem systemów komputerowych;
- przestępstwa związane z treścią;
- przestępstwa związane z naruszeniem praw autorskich i pokrewnych.

Druga kategoria związana jest z metodą popełnienia przestępstwa, a pozostałe nawiązują do przedmiotu ochrony. W tym miejscu należy też odnieść się do stanowiska Rady ds. *Cybercrime Convention*, która w 2006 roku w swoim Raporcie doprecyzowała definicję systemu komputerowego, znajdującą się w art. 1 Konwencji. Pierwotnie był on definiowany jako urządzenie albo grupa urządzeń, które automatycznie przetwarzają dane. Rada jednak w odpowiedzi na rozwój technologiczny podkreśliła, że jako system komputerowy powinno się też traktować wszelkie urządzenia przetwarzające dane, nie tylko komputery. Ponadto, dostarczyła definicji danych komputerowych, określając je jako jakąkolwiek formę przedstawienia faktów czy informacji w postaci, która może być przetwarzana przez program komputerowy.

Wracając jednak do typów przestępstw komputerowych określonych przez Konwencję, należy się pochylić nad każdym z nich z osobna.

Przestępstwa przeciwko spójności i dostępowi do danych i systemów komputerowych, do których odwołuje się Konwencja budapesztańska w art. 2–6, można

[281] Council of Europe – Convention on Cybercrime, ETS No. 185.

określić skrótowo mianem przestępstw związanych z dostępem. Art. 2 Konwencji definiuje niedozwolony dostęp do systemu komputerowego i obliguje państwa-strony do kryminalizowania takiego działania polegającego na celowym uzyskiwaniu dostępu do systemu bez uprawnień. Celem tej regulacji jest zapewnienie użytkownikom systemów spokojnego i bezpiecznego dostępu do informacji i gwarancji, że dostęp do tych danych będą miały tylko osoby upoważnione.

Kolejny artykuł Konwencji odnosi się do ochrony danych i kryminalizuje bezprawną ingerencję za pomocą fizycznego działania w niepubliczny przesył danych. Tutaj jednak Konwencja pozostawia w gestii krajów decyzję, czy do popełnienia czynu zabronionego niezbędna jest umyślność.

Artykuły 4 i 5 tejże Konwencji odnoszą się do zakłóceń systemów komputerowych. Zatem prawodawca położył szczególny nacisk na ochronę spójności i prawidłowego działania systemów. Różnica między art. 4 i 5 polega na tym, że ten pierwszy odnosi się do umyślnego bezprawnego usuwania, uszkadzania danych komputerowych, a ten drugi nawiązuje do bezprawnego zakłócania lub utrudniania działania systemów komputerowych w drodze usuwania czy uszkadzania danych.

Ostatni artykuł dotyczący tej kategorii przestępstw wiąże się z kryminalizacją niewłaściwego użycia urządzeń w celu popełnienia przestępstw uderzających w spójność, bezpieczeństwo czy dostęp do systemów komputerowych lub danych. Tutaj jednak karane jest już samo posiadanie i dystrybucja urządzeń służących do takich działań.

Przestępstwa związane z użyciem systemów komputerowych opisane są przez art. 7 i 8 Konwencji budapesztańskiej. Ten pierwszy przepis zobowiązuje kraje-strony do kryminalizowania umyślnego, bezprawnego fałszowania przy pomocy komputera w celu wprowadzenia, zamiany, usunięcia czy stłumienia danych, skutkującego nieprawdziwością informacji. Krajom pozostawiono jednak decyzję co do strony podmiotowej przestępstwa.

Art. 8 Konwencji, również związany z fałszowaniem przy użyciu komputera, zobowiązuje się do kryminalizowania bezprawnego i umyślnego powodowania utraty własności poprzez wprowadzenie, zamianę, usunięcie czy tłumienie danych bądź inny wpływ na system komputerowy. Jest to przepis o szczególnej doniosłości prawnej, gdyż znaczna część działań przestępnych w cyberprzestrzeni spełnia te przesłanki. Celem tej regulacji jest

zatem ochrona prawa własności, identycznie jak przy zwykłej kryminalizacji kradzieży.

Trzecia i czwarta kategoria ukonstytuowana przez Konwencję nie pozostaje w związku z przedmiotem opracowania, gdyż nawiązuje do przestępstw związanych z treścią oraz prawami autorskimi i im pokrewnymi. Przestępstwo pornografii nieletnich czy naruszenie praw autorskich nie pozostają w związku z opracowaniem przeciwdziałania i reagowania na przestępczość komputerową w instytucjach finansowych.

Opisana wyżej Konwencja stanowi kluczowy akt prawny dla kryminalizacji *cybercrimes*. Była pierwszą międzynarodową odpowiedzią na problem przestępczości komputerowej. O jej szczególnej roli świadczy fakt, że choć uchwaliła ją Rada Europy, to została ratyfikowana przez Stany Zjednoczone Ameryki Północnej w 2006 roku. Polska stała się krajem-stroną Konwencji w 2015 roku[282].

Krajowy porządek prawny zawiera przepisy dotyczące *cybercrimes* w Kodeksie karnym. To krótkie wprowadzenie zostanie jednak ograniczone w zgodzie z przedstawionym wyżej podziałem. Zatem omówione zostaną wyłącznie te przestępstwa, które pozostają w związku z przestępczością w ramach instytucji finansowych.

Pierwszym przepisem, w kolejności ustalonej przez ustawodawcę, Kodeksu karnego dotyczącym *cybercrimes* jest art. 190a § 2 k.k.[283] Odnosi się on do zjawiska *phishingu*, który polega na pozyskaniu poufnych danych osobistych dzięki podszyciu się pod osobę albo instytucję godną zaufania poprzez udostępnienie repliki stron internetowych przypominających autentyczne[284]. Przestępstwo to ma charakter formalny, zatem do jego zaistnienia dochodzi już w momencie podszycia się pod inną osobę czy podmiot[285]. Ponadto,

[282] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie 23 listopada 2001 r. (Dz.U. 2015 r., poz. 728).

[283] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 Nr 88, poz. 553 z późn. zm.).

[284] Binational Working Groupon Cross-Border Mass Marketing Fraud, Report on Phishing. *A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States* (2006), s. 4.

[285] Art. 190a k.k. nb. 12, https://www.ksiegarnia.beck.pl/17775-kodeks-karny-komentarz-alicja-grzeskowiak [dostęp: 31.05.2019].

przestępstwo to ma charakter kierunkowy, więc czynności sprawcze muszą mieć na celu wyrządzenie szkody majątkowej i osobistej[286].

Kolejnym przestępstwem, który przewiduje polski Kodeks karny, jest nielegalne uzyskanie dostępu do informacji. Zgodnie z tym przepisem, każdy, kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do 2 lat. Na podstawie tego przepisu karze podlega też ten, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego oraz ten, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Ujawnienie takiej informacji innej osobie również stanowi okoliczność uzasadniającą odpowiedzialność karną na gruncie tego przepisu.

Odpowiedzialność karną na podstawie art. 268 k.k. za niszczenie informacji ponosi każdy, kto nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią. W zależności od skutku takiej działalności może on być dotknięty różną dolegliwością sankcji. Jest to przestępstwo materialne, zatem skutkowe, i wymaga winy umyślnej sprawcy.

Art. 268a prawa karnego, będący implementacją Konwencji budapesztańskiej, konstytuuje odpowiedzialność za spowodowanie szkody w bazach danych. Jest to przestępstwo powszechne, zatem może je popełnić każdy, kto wypełni znamiona typu czynu zabronionego. Ponadto, jest przestępstwem skutkowym, zatem przypisanie odpowiedzialności karnej jest uzależnione od wystąpienia rzeczywistej szkody w bazie danych. Rzecz jasna, jeśli chodzi o stronę podmiotową przestępstwa, jest to przestępstwo umyślne.

Kolejnym artykułem pozwalającym na pociągnięcie do odpowiedzialności karnej za *cybercrimes* w związku z działalnością instytucji finansowych jest art. 269a k.k. Każdy, kto nie jest uprawniony i w drodze transmisji, zniszczenia, usunięcia, uszkodzenia, utrudnienia dostępu lub zmiany danych

[286] *Ibidem*, nb. 13.

informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Dla przypisania odpowiedzialności karnej, podobnie jak w wyżej zarysowanym przykładzie, niezbędna jest wina umyślna i wystąpienie skutku przestępnego.

Polski ustawodawca w dalszej części k.k. przewiduje też odpowiedzialność za bezprawne wykorzystanie programów i danych. Zgodnie z art. 269b każdy, kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa komputerowego, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. Przestępstwo ma zatem charakter skutkowy, a przypisanie winy wymaga umyślności sprawcy.

Podlega też odpowiedzialności karnej, na podstawie art. 287 k.k. każdy, kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych. W zależności od skali szkody prawodawca różnicuje tę odpowiedzialność. Wprowadzenie tego przepisu, pomimo penalizowania oszustwa, było niezbędne z uwagi na możliwość istnienia anonimowych poszkodowanych, co uniemożliwiałoby przypisanie odpowiedzialności na podstawie art. 286 k.k. Jest to przestępstwo kierunkowe i dla zaistnienia odpowiedzialności nie wymaga skutku, zatem w połączeniu z oderwaniem odpowiedzialności od poszkodowanego może być łatwiej przypisywane potencjalnym sprawcom.

Jeżeli zaś chodzi o prawodawstwo zagraniczne związane ze zjawiskiem *cybercrimes*, które może stanowić inspirację dla polskiego prawodawcy, to przedstawia się ono następująco:

6.1. Niemcy[287]

6.1.1. Hakerstwo (tj. nieuprawniony dostęp)

Hakerstwo stanowi przestępstwo w rozumieniu § 202a niemieckiego Kodeksu karnego[288] (tzw. „nieuprawnione uzyskiwanie danych"). Zgodnie z tym przepisem każdy, kto bezprawnie uzyska dane dla siebie lub dla innej osoby, które nie były dla niego przeznaczone i były szczególnie chronione przed nieuprawnionym dostępem, jeżeli ominął ochronę, podlega karze pozbawienia wolności do lat trzech lub karze grzywny.

6.1.2. Ataki typu *denial-of-service*

Ataki typu *denial-of-service* stanowią przestępstwo zgodnie z § 303b niemieckiego Kodeksu karnego (tzw. sabotaż komputerowy). Zgodnie z tym przepisem każdy, kto zakłóca operacje przetwarzania danych, które mają istotne znaczenie dla innej osoby poprzez usunięcie, zatajenie, uczynienie bezużytecznymi lub zmianę danych, lub poprzez wprowadzanie lub przekazywanie danych z zamiarem wyrządzenia szkody innej osobie, podlega karze pozbawienia wolności do lat trzech lub karze grzywny.

To samo dotyczy niszczenia, uszkadzania, unieszkodliwiania, usuwania lub zmiany systemu przetwarzania danych lub nośnika danych. Należy również zauważyć, że sama próba jest karalna i jeżeli operacja przetwarzania danych ma istotne znaczenie dla innego przedsiębiorstwa lub organu publicznego, jako karę przewiduje się pozbawienie wolności do lat pięciu lub grzywnę. Te same przepisy stosuje się do przestępstwa zakażenia systemów informatycznych złośliwym oprogramowaniem.

---

[287] Opracowane w oparciu o International Comparative Legal Guides, *Cybersecurity 2018*, https://acceurope2018.com/resources/20/The-International-Comparative-Legal-Guide-to--Cybersecurity-2018-1st-Edition.pdf [dostęp: 13.05.2019], s. 61–66.

[288] Strafgesetzbuch (StGB).

6.1.3. *Phishing*

Phishing może stanowić dwa różne przestępstwa kryminalne. Bezprawne przechwytywanie danych za pomocą środków technicznych z niepublicznego podmiotu przetwarzającego dane stanowi przestępstwo zgodnie z § 202b niemieckiego Kodeksu karnego i jest zagrożone karą pozbawienia wolności do dwóch lat lub karą grzywny. Wykorzystanie takich danych w celu uzyskania niezgodnej z prawem korzyści materialnej stanowiłoby przestępstwo w rozumieniu § 263a niemieckiego Kodeksu karnego (tzw. „oszustwo komputerowe") i podlega karze pozbawienia wolności do lat pięciu lub grzywnie.

6.1.4. Posiadanie lub używanie sprzętu, oprogramowania lub innych narzędzi wykorzystywanych do popełnienia cyberprzestępczości (np. narzędzi hakerskich)

Posiadanie sprzętu, oprogramowania lub innych narzędzi, które mogą być wykorzystane do popełnienia cyberprzestępczości, może stanowić przestępstwo zgodnie z § 202c niemieckiego Kodeksu karnego. Zgodnie z tym przepisem przygotowanie do nieuprawnionego uzyskania danych lub *phishingu* poprzez produkcję, nabywanie dla siebie lub innej osoby, sprzedaż, dostarczanie, rozpowszechnianie lub udostępnianie oprogramowania w inny sposób w celu popełnienia takiego przestępstwa podlega karze pozbawienia wolności do jednego roku lub grzywnie. W przypadku stosowania takich instrumentów stosuje się te same zasady, które zostały określone powyżej w odniesieniu do hakerstwa.

6.1.5. Kradzież tożsamości lub oszustwo tożsamości (np. w związku z urządzeniami dostępowymi)

Kradzież tożsamości może stanowić różne przestępstwa, w zależności od tego, w jaki sposób sprawca uzyskuje dostęp do danych dotyczących tożsamości. Można tego dokonać albo poprzez *phishing*, który zgodnie z § 202b niemieckiego Kodeksu karnego stanowiłby przestępstwo, albo poprzez wykorzystanie danych dotyczących tożsamości w celach oszukańczych, które

zgodnie z § 263 niemieckiego Kodeksu karnego (nadużycie finansowe) lub § 263a niemieckiego Kodeksu karnego (oszustwo komputerowe) mogłoby stanowić przestępstwo karne; w przypadku obu tych rodzajów przestępstw grozi kara pozbawienia wolności do 10 lat.

6.1.6. *Electronic theft*

Stanowi przestępstwo jedynie na warunkach określonych w § 202a niemieckiego Kodeksu karnego. Dane, których to dotyczy, muszą być szczególnie chronione przed nieuprawnionym dostępem. Zwykle nie ma to miejsca w przypadku, gdy obecny lub były pracownik narusza zaufanie, ponieważ ma on prawo dostępu do danych. Jeśli tak nie jest, a pracownik obchodzi ochronę, stanowi to przestępstwo *phishingu*. Zastosowanie miałyby wyżej wymienione zasady.

6.1.7. Każda inna działalność, która negatywnie wpływa lub zagraża bezpieczeństwu, poufności, integralności lub dostępności jakiegokolwiek systemu informatycznego, infrastruktury, sieci komunikacyjnej, urządzenia lub danych

Zgodnie z niemieckim prawem karnym niektóre inne działania związane z wyżej wymienionymi przestępstwami stanowią przestępstwa kryminalne. Są to:

(i) przygotowanie nieuprawnionego uzyskania lub przechwycenia danych, art. 202c niemieckiego Kodeksu karnego;
(ii) postępowanie z danymi skradzionymi, art. 202d niemieckiego Kodeksu karnego;
(iii) naruszenie tajemnicy pocztowej i telekomunikacyjnej, art. 206 niemieckiego Kodeksu karnego;
(iv) sabotaż komputerowy, art. 303b niemieckiego Kodeksu karnego;
(v) niektóre rodzaje naruszeń ogólnego rozporządzenia UE o ochronie danych z zamiarem wzbogacenia lub zaszkodzenia komuś, art. 84 ogólnego rozporządzenia o ochronie danych i art. 42 niemieckiej federalnej ustawy o ochronie danych;

(vi) fałszowanie dowodów cyfrowych, art. 269 i następne niemieckiego Kodeksu karnego.

6.1.8. Niewdrożenie przez organizację środków bezpieczeństwa cybernetycznego

Niewdrożenie przez organizację środków bezpieczeństwa cybernetycznego nie jest przestępstwem karnym, lecz administracyjnym, a organizacja podlegałaby odpowiedzialności cywilnej w przypadku zaniedbania. Kara pieniężna może wynieść do 10 mln EUR lub 2% rocznych obrotów przedsiębiorstwa.

Jeżeli chodzi o szczegółowe regulacje dotyczące wyłącznie instytucji finansowych, to należy zwrócić uwagę na art. 25a niemieckiego prawa bankowego (*Kreditwesengesetz*). Ustawa ta, będąca implementacją dyrektywy 98/26/EC, nakłada na instytucje finansowe obowiązek stworzenia wewnętrznej struktury zarządzania ryzykiem i zgodności w celu przeciwdziałania wszelkim nieprawidłowościom w ramach prowadzonej działalności, w tym potencjalnym przestępstwom komputerowym. Polskim odpowiednikiem tego przepisu jest art. 9a ustawy prawo bankowe.

6.2. Włochy[289]

6.2.1. Nieuprawniony dostęp do komputera lub systemu telekomunikacyjnego (art. 615 ter, Kodeks karny[290])

Przestępstwo to wymaga od osoby uzyskania dostępu do chronionej informacji lub systemu telekomunikacyjnego wbrew wyraźnej lub dorozumianej zgodzie osoby uprawnionej na uzyskanie takiego dostępu. Karą jest pozbawienie wolności do lat trzech.

[289] Opracowane w oparciu o: International Comparative Legal Guides, *Cybersecurity 2018*, s. 97–103.

[290] Codice penale italiano, *Regio decreto 19 ottobre 1930*, n. 1398.

6.2.2. Oszustwo cyfrowe (art. 640 ter, Kodeks karny)

Przestępstwo to ma miejsce wtedy, gdy ktokolwiek świadomie i z zamiarem oszukania manipuluje przy jednym lub większej liczbie urządzeń cyfrowych, nielegalnie wykorzystując informacje, dane lub oprogramowanie na urządzeniu cyfrowym, w celu zdobycia pieniędzy i zaszkodzenia komuś innemu. Karą jest pozbawienie wolności na okres od sześciu miesięcy do trzech lat.

6.2.3. Fałszowanie tożsamości (art. 494, Kodeks karny)

Przedmiotowy artykuł ma zastosowanie zarówno do prawdziwych tożsamości, jak i tożsamości cyfrowych; dane przestępstwo jest popełniane, gdy ktoś fałszywie i umyślnie przedstawia się jako ktoś inny. Karą jest pozbawienie wolności do roku.

6.2.4. Nielegalne posiadanie i rozpowszechnianie haseł do systemów cyfrowych (art. 615 quater, Kodeks karny)

Przestępstwo to popełniane jest wtedy, gdy osoba nielegalnie posiada lub rozpowszechnia tajne kody dostępu, w celu zdobycia pieniędzy lub zaszkodzenia komuś innemu. Karą jest pozbawienie wolności do jednego roku.

6.2.5. Uszkodzenie informacji cyfrowych, danych lub oprogramowania (art. 635 bis, Kodeks karny)

Dzieje się tak, gdy ktoś celowo uszkadza, niszczy, usuwa lub wyłącza wszelkiego rodzaju informacje cyfrowe, dane lub oprogramowanie należące do kogoś innego. Karą jest pozbawienie wolności na okres od sześciu miesięcy do trzech lat.

6.2.6. Uszkodzenie informacji cyfrowych, danych lub oprogramowania (art. 635 bis, Kodeks karny)

Posiadanie lub używanie sprzętu, oprogramowania lub innych narzędzi wykorzystywanych do popełnienia cyberprzestępczości (np. narzędzi hakerskich).

6.2.7. Bezprawne ujawnienie tajnych informacji zawodowych (art. 622, Kodeks karny)

Przestępstwo to wymaga od osoby fizycznej celowego ujawnienia innym osobom wszelkich tajnych informacji, które zna ze względu na swój zawód lub pracę. Karą jest pozbawienie wolności do roku.

6.2.8. Bezprawne przechwytywanie i niszczenie komunikacji (art. 616, Kodeks karny)

Przestępstwo to popełniane jest wtedy, gdy osoba otwiera, kradnie lub niszczy korespondencję, w tym pocztę elektroniczną, która nie jest do niej skierowana. Karą jest pozbawienie wolności do jednego roku.

6.2.9. Bezprawne przechwytywanie, zniekształcanie, fałszowanie, niszczenie korespondencji (art. 617, Kodeksu karny)

Te różne przestępstwa, karane kilkoma artykułami są popełniane, gdy osoba otwiera, kradnie lub niszczy korespondencję, w tym e-maile, które nie są do niej adresowane, nawet przy użyciu oprogramowania, złośliwego oprogramowania lub innego rodzaju narzędzi cyfrowych mających jeden z tych celów. Karą jest pozbawienie wolności na okres od sześciu miesięcy/jeden rok do czterech lat.

6.2.10. Bezprawne ujawnienie korespondencji (art. 618, Kodeks karny)

Przestępstwo to popełniane jest wtedy, gdy osoba umyślnie ujawnia lub usiłuje ujawnić jakiejkolwiek innej osobie treść jakiejkolwiek korespondencji przewodowej, ustnej lub elektronicznej, wiedząc lub mając powody, aby wiedzieć, że informacja została uzyskana poprzez przechwycenie informacji przewodowej, ustnej lub elektronicznej, z naruszeniem tego przepisu. Karą jest pozbawienie wolności do sześciu miesięcy.

Jeżeli chodzi o szczegółowe regulacje dotyczące *cybercrimes*, to ustawa nr 48/2008, która ratyfikowała Konwencję budapeszteńską z 2001 r. o cyberprzestępczości, zaktualizowała zarówno Kodeks ochrony danych, jak i dekret ustawodawczy nr 231/2001[291] oraz wprowadziła odpowiedzialność karną przedsiębiorstw w związku z cyberprzestępczością i przestępstwami komputerowymi popełnianymi w interesie firmy. Firmy mogą jednak chronić się przed odpowiedzialnością wynikającą z popełnienia przestępstwa, jeżeli m.in. przed popełnieniem przestępstwa przyjmą i skutecznie wdrożą model zgodności (*compliance*) mający na celu zapobieganie przestępstwom tego samego rodzaju, co przestępstwo popełnione.

Szczególną rolę pełni też wtórne prawodawstwo. Circular No. 285 of 17 December 2013 wydany przez Bank Centralny Włoch konstytuuje jego uprawnienie do bycia powiadomionym o nieprawidłowościach w przetwarzaniu danych w ramach systemu finansowego.

6.3. Chiny[292]

Głównym źródłem regulacji cyberprzestępstw w Kodeksie karnym Chińskiej Republiki Ludowej[293] jest sekcja „Zbrodnie zakłócające porządek publiczny". Artykuły 285, 286 i 287 to trzy główne artykuły bezpośrednio

[291] Decreto Legislativo 8 giugno 2001, n. 231, Disciplina della responsabilita' amministrativa delle persone giuridiche, delle societa' e delle associazioni anche prive di personalita' giuridica, a norma dell'articolo 11 della legge 29 Settembre 2000, n. 300.

[292] Opracowane w oparciu o: International Comparative Legal Guides, *Cybersecurity 2018*, s. 33–39.

[293] Order of the President of The People's Republic of China, No. 83.

ich dotyczące. Ponadto art. 253 ust. 1 pośrednio odnosi się do cyberbezpieczeństwa i ma zastosowanie do aktów naruszenia informacji osobistych w internecie. Katalog kar za naruszenie artykułów 285, 286 i 287 obejmuje karę pozbawienia wolności, aresztu i grzywny. Na przykład sprawca w poważnych przypadkach może zostać skazany na maksymalnie siedem lat więzienia za nielegalne pozyskanie danych z komputerowego systemu informatycznego.

Warto zauważyć, że artykuły 286 i 287 ustanawiają zasadę, że jeśli ktoś używa komputerów (np. poprzez hakowanie, wyłudzanie informacji lub inne nielegalne działania powiązane z internetem), popełnia inne przestępstwa (tj. przestępstwa, które tradycyjnie nie miały związku z internetem), takie jak: oszustwa finansowe, kradzieże, sprzeniewierzenie, sprzeniewierzenie funduszy publicznych i kradzież tajemnic państwowych, zostanie skazany za przestępstwo, za które jest cięższa kara.

6.3.1. Hakerstwo (tj. nieautoryzowany dostęp)

Zgodnie z art. 285 k.k. działania polegające na ataku na komputerowy system informacyjny w obszarach spraw państwowych, obrony narodowej lub zaawansowanej nauki i techniki stanowią *przestępstwo polegające na ataku na komputerowy system informacyjny*. Przestępca zostaje skazany na karę pozbawienia wolności w wymiarze nie krótszym niż trzy lata. W przypadku działań polegających na ataku na komputerowy system informacyjny, inny niż w powyższych obszarach, może stanowić *przestępstwo polegające na uzyskiwaniu danych z komputerowego systemu informacyjnego i przejęcia kontroli nad komputerowym systemem informacyjnym*, a sprawca zostaje skazany na karę pozbawienia wolności na czas określony – nie więcej niż trzy lata lub pozbawienia wolności lub karę więzienia od trzech do siedmiu lat w poważnych przypadkach. Jeśli podmiot gospodarczy popełni te przestępstwa, zostanie ukarany grzywną, a osoby bezpośrednio odpowiedzialne i inne osoby odpowiedzialne za popełnienie przestępstwa zostaną odpowiednio ukarane.

6.3.2. Ataki wykorzystujące odmowę dostępu

Zgodnie z art. 286 Kodeksu karnego ChRL, tego typu ataki mogą stanowić *przestępstwo sabotowania komputerowego systemu informacyjnego*, a w poważnych przypadkach wiążą się z karą ponad pięciu lat więzienia.

6.3.3. Wyłudzanie informacji

Phishing jest zwykle przeprowadzany w celu kradzieży lub w inny sposób pozyskiwania danych osobowych obywateli, co jest uważane za *przestępstwo polegające na naruszeniu danych osobowych obywatela*, o którym mowa w art. 253 ust. 1, a za które przewiduje się karę nawet do siedmiu lat pozbawienia wolności.

6.3.4. Wprowadzanie do systemów IT złośliwego oprogramowania (w tym oprogramowania szantażującego, szpiegującego i innych)

Na podstawie art. 286 Kodeksu karnego ChRL celowe tworzenie lub rozpowszechnianie wirusów komputerowych lub innych destrukcyjnych programów, mających wpływ na normalne działanie komputerowego systemu informatycznego i powodujących poważne konsekwencje, stanowi *przestępstwo sabotowania komputerowego systemu informacyjnego*. W poważnych przypadkach sprawca może zostać skazany na pięć lat więzienia.

6.3.5. Posiadanie lub używanie sprzętu, oprogramowania lub innych narzędzi wykorzystywanych do popełniania cyberprzestępczości (np. narzędzia hakerskie)

Jeśli ktoś posiada lub używa sprzęt, oprogramowanie lub inne narzędzia do popełnienia cyberprzestępstwa, w zależności od popełnionego przewinienia, sprawca może zostać *skazany za przestępstwo ataku na komputerowy system informacyjny*.

Istnieje również przestępstwo *nielegalnego korzystania z sieci informacyjnych*, które obejmuje korzystanie z sieci informacyjnej w celu tworzenia stron internetowych i grup komunikacyjnych do działań przestępczych, takich jak: oszustwo, nauczanie metod kryminalnych, produkcja lub sprzedaż przedmiotów czy substancji zabronionych. W przypadku, gdy działanie stanowi więcej niż jedno przestępstwo, winowajca zostanie skazany za przestępstwo, które nałoży na niego surowszą karę.

6.3.6. Kradzież tożsamości

Zgodnie z chińskim Kodeksem karnym w przypadku kradzieży tożsamości, jeśli przestępca uzyska tożsamość poprzez kradzież lub w inny sposób nielegalnie nabywa dane osobowe obywateli, działalność taka może zostać uznana za *przestępstwo polegające na naruszeniu danych osobowych obywatela* zgodnie z art. 253 ust. 1. Jeśli ktoś wykorzystuje skradzioną tożsamość innych osób jako swój własny dowód tożsamości, takie zachowanie może stanowić *przestępstwo kradzieży tożsamości* zgodnie z art. 281; w przypadku, gdy taka osoba wykorzystuje skradzioną tożsamość do popełnienia oszustwa lub innej działalności przestępczej, powinna zostać skazana za przestępstwo, za które grozi surowsza kara.

6.3.7. *Electronic theft*

Jeśli aktualny lub były pracownik naruszy obowiązek poufności i spowoduje naruszenie danych osobowych, tajemnic handlowych, tajemnic państwowych itp., sprawca zostanie skazany zgodnie z art. 287 i ukarany zgodnie z odpowiednimi przepisami prawa karnego (np. za *przestępstwo naruszania tajemnic handlowych*).

6.3.8. Wszelkie inne działania, które negatywnie wpływają na bezpieczeństwo, poufność, integralność lub działanie jakiegokolwiek systemu informatycznego, infrastruktury, sieci komunikacyjnej, urządzenia lub danych

Jeśli ktoś z naruszeniem przepisów ustawowych i wykonawczych, usuwa, zmienia, dodaje lub zakłóca działanie komputerowego systemu informatycznego i powoduje niezdolność systemu informatycznego do normalnego działania lub przeprowadza operacje usunięcia, zmiany lub uzupełnienia danych lub aplikacji, które są przechowywane, usuwane lub przesyłane w systemie informatycznym komputera i powoduje tym poważne konsekwencje, popełnia *przestępstwo sabotowania komputerowego systemu informatycznego* zgodnie z art. 286 k.k. W przypadku spowodowania poważnych konsekwencji sprawca zostanie skazany na karę pozbawienia wolności na czas dłuższy niż pięć lat.

6.3.9. Niepowodzenie organizacji wdrożenia środków bezpieczeństwa cybernetycznego

Zgodnie z art. 286 ust. 1 k.k., jeśli organizacja jest dostawcą usług sieciowych i nie wykonuje prawidłowo swoich obowiązków związanych z zarządzaniem bezpieczeństwem w swojej sieci informacyjnej, przewidzianych w przepisach ustawowych i administracyjnych, i odmawia korygowania swojego postępowania, organizacja zostaje ukarana grzywną, a osoby bezpośrednio odpowiedzialne i inne osoby bezpośrednio odpowiedzialne za przestępstwa mogą zostać skazane na pozbawienie wolności w wymiarze ustalonym na czas nie dłuższy niż trzy lata, w następujących okolicznościach:

(1) rozpowszechniania dużej ilości nielegalnych informacji;
(2) ujawnienia informacji o użytkowniku, powodujące poważne konsekwencje;
(3) spowodowania uszkodzenia lub utraty dowodów karnych, co pociąga za sobą poważne konsekwencje;
(4) w przypadku innych poważnych okoliczności.

Na mocy obowiązujących przepisów lub w drodze dyspozycji organów regulacyjnych organizacjom stawia się także szczególne wymogi zgłaszania

informacji dotyczących możliwości zaistnienia lub zaistnienia incydentów organowi regulacyjnemu lub innemu. Należą do nich:

(a) Obowiązek raportowania rodzi się w momencie wystąpienia zagrożenia bezpieczeństwa sieci;
(b) Zgodnie z *Cybersecurity Law* i odpowiednimi przepisami operatorzy sieci informują co najmniej samorząd lokalny, organ regulacyjny sektora przemysłu i lokalną administrację cyberprzestrzeni. Zgodnie z *Regulations of the People's Republic of China on the Security Protection of Computer Information System* wszelkie przypadki zagrożeń są zgłaszane organowi bezpieczeństwa publicznego w ciągu 24 godzin.
(c) Zgłoszeniu podlegają co najmniej: informacja o stronie powiadamiającej; opis sytuacji zagrożenia bezpieczeństwa sieci; szczegółowe informacje o sytuacji; charakter incydentu; informacje o dobrach dotkniętych zagrożeniem; informacje o danych osobistych, które mogły zostać dotknięte atakiem; opis podjętych jak dotąd działań; wstępna ocena zakresu strat poniesionych wskutek ataku;
(d) Publikacja informacji związanych z incydentem jest zabroniona, gdy zagraża bezpieczeństwu narodowemu lub interesowi publicznemu.

Zgodnie *Cybersecurity Law* władze wspierają współpracę operatorów sieci w zakresie gromadzenia, analizowania i powiadamiania o zagrożeniach cyberbezpieczeństwa i reagowania w sytuacjach kryzysowych w celu zwiększenia ich zdolności do ochrony cyberbezpieczeństwa.

W Chinach zachęca się użytkowników, dostawców i instytucje badawcze do zgłaszania wszelkich potencjalnych słabości systemów do Chińskiej Bazy Danych Bezpieczeństwa Narodowego w celu zebrania, weryfikacji i ostrzeżenia przed różnorakimi zagrożeniami i ustanowienia skutecznego i skoordynowanego mechanizmu reagowania kryzysowego wśród wszystkich operatorów.

Jeśli chodzi o różnice w wymogach stawianych organizacjom, to w zależności od branży, w której one działają, istnieją pewne szczególne regulacje dotyczące gromadzenia i ochrony informacji, zapobiegania wyciekom informacji i reagowania w sytuacjach kryzysowych na te zdarzenia. Co do zasady jednak stoją one w zgodzie z uregulowaniami przewidzianymi przez *Cybersecurity*

Law. Jako przykład takiej szczególnej regulacji może posłużyć *Provisional Rules on Management of the Individual Credit Information Database* – jest to akt ogłaszany przez Bank Ludowy Chin w celu zapewnienia bezpiecznego i zgodnego z prawem wykorzystania osobistych informacji kredytowych.

6.4. Australia[294]

6.4.1. Hakerstwo

W Nowej Południowej Walii w Australii nieautoryzowany dostęp do systemów komputerowych jest kryminalizowany zarówno przez ustawodawstwo stanowe, jak i federalne, a mianowicie Crimes Act 1900[295] (NSW) oraz Commonwealth Criminal Code[296]. Najczęściej osoby podejrzane o popełnienie cyberprzestępczości są oskarżane zgodnie z Kodeksem, ze względu na jego powszechne zastosowanie we wszystkich stanach i terytoriach Australii.

Osoby podejrzane o nieuprawniony dostęp do systemów komputerowych są oskarżane na podstawie art. 478.1 Kodeksu, który przewiduje przestępstwo *nieuprawnionego dostępu do danych lub ich modyfikacji*. Na przestępstwo składają się trzy elementy dowodowe. Przestępstwo jest popełniane, jeżeli osoba zyskuje nieuprawniony dostęp do danych zastrzeżonych lub ich modyfikację, osoba ta zamierza spowodować dostęp lub modyfikację, wiedząc, że dostęp lub modyfikacja danych są nieuprawnione. Maksymalną karą za naruszenie powyżej opisanej normy Kodeksu jest kara dwóch lat pozbawienia wolności.

6.4.2. Ataki typu *denial-of-service* (wykorzystujące odmowę dostępu)

Ataki typu *denial-of-service* („ataki typu DoS") lub *Distributed Denial of Service* („ataki typu DDoS") są kryminalizowane przez s. 477.3 Kodeksu, który przewiduje *przestępstwo nieuprawnionego uszkodzenia komunikacji elektronicznej*. Przestępstwo składa się z dwóch elementów. Przestępstwo jest popełniane,

---

[294] Opracowane w oparciu o: International Comparative Legal Guides, *Cybersecurity 2018*, s. 22–27.

[295] Crimes Act 1900 No. 40.

[296] Criminal Code Act 1995 No. 12, 1995 z późn. zm.

jeżeli osoba powoduje jakiekolwiek nieuprawnione uszkodzenie komunikacji elektronicznej kierowanej do lub z komputera, wiedząc, że działanie takie jest nieuprawnione. Maksymalna kara za naruszenie normy to 10 lat pozbawienia wolności.

6.4.3. *Phishing*

Phishing, będący formą oszustwa internetowego, jest kryminalizowany zarówno przez *Crimes Act*, jak i przez Kodeks. Jednak egzekwowanie przepisów dotyczących oszustw internetowych pozostawia się zazwyczaj organom ścigania państwa, w którym zamieszkuje ofiara oszustwa. W Nowej Południowej Walii oszustwo jest kryminalizowane przez s. 192E ustawy o przestępstwach (*Crimes Act*). Przestępstwo jest popełniane, jeśli osoba, która przez oszustwo nieuczciwie nabywa mienie należące do innej osoby lub powoduje pogorszenie sytuacji finansowej. Maksymalna kara to 10 lat pozbawienia wolności.

6.4.4. Zakażenie systemów informatycznych złośliwym oprogramowaniem (w tym oprogramowaniem typu *ransomware*, *spyware*, robaki, trojany i wirusy)

Zakażenie systemów informatycznych złośliwym oprogramowaniem jest karane przez s. 478.2 Kodeksu, który przewiduje przestępstwo *Nieuprawnionego uszkodzenia danych przechowywanych na dysku komputera*. Przestępstwo składa się z trzech elementów. Przestępstwo jest popełniane, jeżeli osoba powoduje nieuprawnione pogorszenie wiarygodności, bezpieczeństwa lub działania danych przechowywanych na dysku komputera, karcie kredytowej, innym urządzeniu służącym do przechowywania danych drogą elektroniczną, a osoba ta zamierza spowodować uszkodzenie, wiedząc, że jest ono bezprawne. Maksymalna kara to dwa lata pozbawienia wolności.

6.4.5. Posiadanie lub używanie sprzętu, oprogramowania lub innych narzędzi służących do popełnienia cyberprzestępczości (np. narzędzi hakerskich)

Posiadanie lub używanie sprzętu, oprogramowania lub innych narzędzi wykorzystywanych do popełnienia cyberprzestępczości jest karalne przez s. 478.3 Kodeksu, który przewiduje przestępstwo posiadania lub kontroli danych z zamiarem popełnienia przestępstwa komputerowego. Przestępstwo składa się z dwóch elementów. Przestępstwo jest popełniane, jeżeli osoba posiada lub kontroluje dane z zamiarem wykorzystania danych przez siebie lub inną osobę, popełniając przestępstwo przeciwko działowi 477 Kodeksu lub ułatwiając popełnienie takiego przestępstwa. Maksymalna kara za naruszenie s. 478.3 Kodeksu to trzy lata kary więzienia.

6.4.6. Kradzież tożsamości

Przestępstwa związane z tożsamością, a w szczególności przestępstwa związane z fałszowaniem tożsamości, są kryminalizowane przez dział 372 Kodeksu. Szczególne czyny, które są kryminalizowane, obejmują: postępowanie z danymi identyfikującymi, także postępowanie z takimi informacjami, gdy wiążą się one z korzystaniem z usług przewozowych, posiadaniem informacji identyfikujących oraz posiadaniem sprzętu używanego do sporządzania danych identyfikujących.

6.4.7. *Electronic theft*

Przestępstwo to jest kryminalizowane przez s. 478.1 Kodeksu. Przestępstwo jest popełniane, jeżeli osoba modyfikuje dane zastrzeżone. Modyfikacja jest zdefiniowana w Kodeksie jako zmiana lub usunięcie danych przechowywanych w komputerze lub dodanie treści do danych już przechowywanych w komputerze, nieuprawnione kopiowanie danych z komputera również byłoby naruszeniem przepisów prawnokarnych.

6.4.8. Niewdrożenie przez organizację środków bezpieczeństwa cybernetycznego

Aktem mającym znaczenie dla zwalczania zagrożeń cybernetycznych jest The Security of Critical Infrastructure Act 2018 (Cth)[297]. Wszedł w życie 11 lipca 2018 r., ma na celu zarządzanie zagrożeniami dla bezpieczeństwa narodowego w postaci sabotażu, szpiegostwa i przymusu ze strony podmiotów zagranicznych. Został wdrożony w odpowiedzi na zmiany technologiczne, które zwiększyły możliwości łączenia z infrastrukturą krytyczną. Ustawodawca australijski wyszedł z założenia, że odpowiedzialność za zapewnienie ciągłości działania i świadczenie podstawowych usług dla australijskiej gospodarki i społeczności leży po stronie zarówno właścicieli i operatorów infrastruktury krytycznej, jak i władz terytorialnych oraz rządu australijskiego.

The Australian Securities and Investments Commission (ASIC) zapewnia wytyczne dla australijskich zintegrowanych rynków korporacyjnych, usług finansowych i regulatorów rynku konsumenckiego, a także dostarcza wskazówek dla organizacji poprzez swoje „cyber reliance good practices". Dobre praktyki zalecają m.in. okresowy przegląd strategii cybernetycznej przez radę dyrektorów, wykorzystanie odporności cybernetycznej jako narzędzia zarządzania, dostosowanie ładu korporacyjnego (tj. aktualizacja polityki i procedur w zakresie bezpieczeństwa cybernetycznego), współpracę i wymianę informacji, zarządzanie ryzykiem przez osoby trzecie oraz wdrażanie systemów stałego monitorowania.

Regulacją ważną w sektorze finansowym jest Privacy Act[298]. Jedna z jego części (IIIA) reguluje w szczególności przetwarzanie danych osobowych dotyczących działalności osób fizycznych w związku z kredytem konsumenckim, w tym rodzajów danych osobowych, które kredytodawcy mogą ujawnić. Wszystkie organy sprawozdawczości kredytowej (zdefiniowane w pkt 6 i 6P jako podmioty gospodarcze, których działalność polega na zbieraniu, przechowywaniu, wykorzystywaniu lub ujawnianiu danych osobowych osób fizycznych w celu dostarczenia podmiotowi informacji o zdolności kredytowej osoby fizycznej) podlegają przepisom części III.

---

[297] Security of Critical Infrastructure Act 2018 No. 29, 2018.

[298] Privacy Act 1988 No. 119, 1988.

W lutym 2018 r. w ustawie z 2017 r. o zmianie ustawy o ochronie prywatności (*Notifiable Data Breaches*) wprowadzono zmiany w ustawie o ochronie prywatności, tak aby podmioty australijskich zasad ochrony prywatności (APP) były zobowiązane do jak najszybszego powiadomienia OAIC (*The Office of the Australian Information Commissioner*) oraz aby osoby fizyczne zostały powiadomione o naruszeniu danych osobowych w przypadku, gdy istnieją uzasadnione powody do stwierdzenia, że naruszenie takie miało miejsce. Proces ten nazywany jest Notifiable Data Breaches Scheme.

Powyższej określone naruszenia danych powstają w przypadku: nieuprawnionego dostępu lub nieuprawnionego ujawnienia danych osobowych lub utraty danych osobowych, które posiada dany podmiot; nieuprawnionego ujawnienia danych osobowych lub utraty danych osobowych mogącego spowodować poważną szkodę dla jednej lub więcej osób fizycznych; oraz gdy podmiot nie był w stanie zapobiec prawdopodobnemu ryzyku wystąpienia poważnej szkody poprzez podjęcie działań naprawczych.

OAIC oczekuje, że podmioty APP przeprowadzą szybką ocenę podejrzewanego naruszenia ochrony danych w celu ustalenia, czy może ono spowodować poważną szkodę.

Powiadomienie OAIC i osób, których dotknęło naruszenie, musi zawierać tożsamość i dane kontaktowe organizacji, opis naruszenia ochrony danych, rodzaje informacji pozyskanych przez naruszenie oraz zalecenia dotyczące kroków, jakie osoby fizyczne powinny podjąć w odpowiedzi na naruszenie danych.

Nieprzestrzeganie obowiązku powiadomienia może skutkować nałożeniem znacznych kar cywilnych. Poważna lub powtarzająca się ingerencja w prywatność pociąga za sobą karę grzywny w wysokości 2000 jednostek karnych (*penalty units*), obecnie około 420 000 dolarów australijskich. Maksymalna kara, jaką sąd może nałożyć na osobę prawną, jest pięciokrotnością powyższej kwoty.

6.5. Konkluzje

Rozważając potencjalne udoskonalenia polskiego porządku prawnego w kwestii *cybercrimes*, należałoby się skupić przede wszystkim na wprowadzeniu obowiązkowych komórek wewnętrznych w ramach instytucji finansowych, których zadaniem byłoby przeciwdziałanie i wczesne reagowanie na wszelkie nieprawidłowości w systemach komputerowych. Zdecentralizowana kontrola zgodności z wytycznymi i rekomendacjami związanymi z przeciwdziałaniem przestępczości stanowiłaby niezwykle skuteczny instrument w ograniczaniu przestępczości w instytucjach finansowych[299]. Niezastosowanie się do wymagań ustawowych, rzecz jasna, powinno być skrzętnie egzekwowane[300], a niesubordynacja powinna spotykać się z karami administracyjnymi. Warto też zastanowić się nad zachętą dla instytucji finansowych do wdrożenia takiego programu. Można bowiem stworzyć, wzorem włoskich regulacji, odpowiedni mechanizm prawny, który gwarantowałby takim instytucjom prawnym brak odpowiedzialności jako podmiot zbiorowy, gdy wdrożone zostałyby wszelkie zalecone procedury.

Ponadto, komplementarnym do wskazanego powyżej instrumentu mogłaby być zdecentralizowana kontrola bankowa. Mogłaby ona wiązać się z wspólnymi wysiłkami banków komercyjnych w diagnozowaniu podejrzanych zachowań i wzajemnej wymianie informacji i doświadczeń w tej mierze.

Pożądanym rozwiązaniem w ramach decentralizacji kontroli i prewencji byłoby też odpowiednie edukowanie kadry kierowniczej i klientów o potencjalnych zagrożeniach. Pozwala to bowiem zmniejszyć sito kontroli, przez które nierzadko przechodzą drobne przestępstwa komputerowe. Wsparciem tego rozwiązania mogłyby też być nagrody dla potencjalnych informatorów (wewnętrznych i zewnętrznych) pochodzące od instytucji finansowych. Wzorem rozwiązań ze Stanów Zjednoczonych Ameryki Północnej taka osoba mogłaby być gratyfikowana stosownie do kosztów, których udało się uniknąć dzięki jej pomocy.

[299] Przykładem takiego rozwiązania jest przytoczony przy okazji zarządzania ryzykiem przykład Wielkiej Brytanii.

[300] Wzorem australijskich regulacji przedstawionych powyżej.

Pożądane jest zatem przesunięcie akcentów przeciwdziałania przestępstwom komputerowym na instytucje finansowe. Rozproszenie kontroli w połączeniu z kooperacją instytucji finansowych daje lepsze efekty niż holistyczna struktura kontrolna utworzona na podstawie przepisów powszechnie obowiązujących. Rzecz jasna, takie podmioty powinno być odpowiednio stymulowane do zbudowania wewnętrznych i wspólnych struktur. Nie można też w programie przeciwdziałania przestępczości komputerowej w instytucjach finansowych zapomnieć o roli edukacji, o zagrożeniach działaniami przestępczymi, tak by jak najwięcej niebezpieczeństw udało się wyeliminować już w początkowym stadium prewencji.

Schodząc jednak na poziom przeciwdziałania przestępstwom w drodze działań niesformalizowanych (indywidualnie przez wszystkich pracowników), można nakreślić następujące obszary, które można zoptymalizować.

Pierwszy z nich wiąże się z przestarzałą infrastrukturą systemową banków o ugruntowanej pozycji rynkowej. Z uwagi na konieczność ciągłej obsługi transakcji klienta niezwykle trudno diametralnie zmodernizować systemy informatyczne takich podmiotów operujących na rynku finansowym. Zaleca się zatem tworzenie nowego równoległego systemu obsługi, a następnie, po jego odpowiednim opracowaniu, stopniowe wprowadzenie nowych klientów na tę platformę. Ta potrzeba jest niezwykle paląca, gdyż to niedostosowane do wyzwań współczesności systemy bankowe stanowią furtkę dla ataków cybernetycznych.

Kolejnym problemem, z którym należy się zmierzyć, są niewystarczająco zaszyfrowane hasła pracowników instytucji. Rekomenduje się zapewnienie im odpowiednich programów szyfrujących, w celu ograniczenia ryzyka przejęcia ich kont w ramach intranetu.

W powiązaniu z tym problemem pozostaje kwestia wymogu odpowiednio częstych aktualizacji oprogramowania. Nieaktualne oprogramowanie systemowe tworzy równie niebezpieczne ryzyko występowania przestępstw cybernetycznych, co nieaktualny pod względem oprogramowania wewnętrzny informatyczny system bankowy.

Ostatnim elementem, kluczowym już raczej z perspektywy represji niż prewencji, jest zapewnienie odpowiedniego dostępu do kompetentnej osoby w razie wystąpienia ataku. Odpowiednia i szybka reakcja pozwala bowiem

na ograniczenie, a czasem nawet uniknięcie szkód w drodze wystąpienia działania przestępnego.

Te wszystkie działania, których celem jest ograniczenie ryzyka wystąpienia przestępstw komputerowych, osadzone są fundamencie informacji. Nie można skutecznie wdrożyć odpowiednich praktyk, jeśli nie wesprze się ich należytą edukacją pracowników. W tej mierze na barkach instytucji finansowych leży wyzwanie o największym ciężarze gatunkowym. To regularne i użyteczne szkolenia pracowników stanowią niezbędny element skutecznego przeciwdziałania przyczynom przestępczości na rynku finansowym.

ROZDZIAŁ SIÓDMY

Analiza działalności międzynarodowych grup przestępczych oraz metod zapobiegania im w instytucjach finansowych

Kwestia przestępczości, choć mogłaby wydawać się jedynie zjawiskiem o charakterze lokalnym, związanym granicami państw, urasta bez cienia wątpliwości do rangi jednej z głównych przeszkód związanych z procesami globalizacyjnymi. Ryzyko, jakie stanowi zorganizowana przestępczość międzynarodowa, przybiera nieprzerwanie na sile w związku z wprowadzaniem nowych technologii[301]. Członkowie społeczności międzynarodowej zdają się rozumieć znaczenie, jakie ma dla systemu bezpieczeństwa międzynarodowego kwestia międzynarodowej przestępczości finansowej, dlatego podejmują działania mające na celu wykształcenie wspólnych instrumentów zwalczania i zapobiegania istnieniu międzynarodowych grup przestępczych. Rozwój globalnego rynku finansowego w połączeniu z zastosowaniem nowych technologii łączności przyczyniły się zarówno do ogólnoświatowego rozwoju ekonomicznego, jak i do rozwoju międzynarodowej przestępczości zorganizowanej[302].

Wydaje się, że pomimo ważnej roli, jaką odgrywają w zapobieganiu i zwalczaniu przestępczości międzynarodowej umowy regionalne i dwustronne, to jednak właśnie umowy wielostronne o charakterze uniwersalnym, obejmujące swym zakresem podmiotowym jak najszerszy krąg państw, mają największe znaczenie dla skutecznego zwalczania przez społeczność międzynarodową przestępczości[303].

---

[301] E.W. Pływaczewski, *Przestępczość zorganizowana*, Warszawa 2011.

[302] J. Bil, M. Kulik, B. Wojdak, J. Bilewicz, A. Jeżyński, *Zorganizowana przestępczość transgraniczna*, Lublin 2015.

[303] I. Gawłowicz, M.A. Wasilewicz, *Międzynarodowa współpraca w walce z przestępczością*, Szczecin 2004.

Na wstępie niniejszego rozdziału należy również poczynić pewne zastrzeżenie. Celem niniejszej pracy jest bowiem dokonanie dogłębnej analizy oraz charakteryzacji przestępstw o charakterze międzynarodowym, którymi zagrożone są instytucje finansowe obecne na polskim rynku finansowym oraz możliwości ograniczenia ryzyka, na które są one narażone. W związku z powyższym zastrzeżeniem niecelowe z punktu widzenia tematu pracy jest analizowanie wszystkich tzw. przestępstw finansowych uregulowanych w polskim Kodeksie karnym oraz ustawach szczegółowych.

W dalszej części pracy omówione zostaną umowy międzynarodowe, akty prawa unijnego oraz ustawy istotne z punktu widzenia międzynarodowych przestępstw finansowych. Następnie analizie poddane zostaną przestępstwa prania pieniędzy, finansowania terroryzmu oraz zagadnienie tzw. cyberprzestępczości i związane z nim czyny przestępne. Wybór omawianych typów czynów zabronionych podyktowany został częstotliwością występowania w związku z nimi elementu transgranicznego i co za tym idzie, międzynarodowym charakterem omawianych przestępstw.

7.1. Umowy międzynarodowe i akty unijne regulujące zagadnienie przestępczości międzynarodowej w związku z instytucjami finansowymi

W świetle uwag poczynionych na temat problemów wiążących się z globalizacją światowej gospodarki nie powinno nikogo dziwić stwierdzenie, że główną rolę w procesie wypracowywania narzędzi mogących posłużyć skoordynowanemu zwalczaniu przestępczości międzynarodowej powinna odgrywać Organizacja Narodów Zjednoczonych jako największa i najbardziej uniwersalna organizacja międzynarodowa naszych czasów. Dla zachowania przejrzystości oraz rzeczowości wywodu główny nacisk przy omawianiu regulacji międzynarodowych poświęconych przestępczości międzynarodowej zostanie położony na akty prawa międzynarodowego wydawane przez Organizację Narodów Zjednoczonych. Oprócz tego przeanalizowane zostaną także najistotniejsze akty prawa wspólnotowego wydane przez organy Unii Europejskiej.

Wydaje się, że najważniejszym aktem prawa międzynarodowego związanym z omawianym zagadnieniem jest Konwencja Narodów Zjednoczonych

przeciwko międzynarodowej przestępczości z Palermo z 2000 roku. W konwencji tej przyjęto szerokie rozumienie przymiotu międzynarodowości danego przestępstwa. Miało to w zamyśle ułatwić organom wymiaru sprawiedliwości zwalczanie międzynarodowej przestępczości, w tym przestępczości finansowej. Artykuł 3, ust. 2 konwencji z Palermo stanowi wymienienie przesłanek, których spełnienie pozwala przypisać danemu czynowi zabronionemu cechę międzynarodowości (*is transnational in nature*), co z kolei umożliwia zastosowanie Konwencji. Zgodnie z omawianym aktem przestępstwo ma charakter międzynarodowy, jeżeli:

- zostało popełnione w więcej niż jednym państwie;
- zostało popełnione w jednym państwie, lecz istotna część przygotowań do niego, planowania, kierowania lub kontroli nad nim odbywała się w innym państwie;
- zostało popełnione w jednym państwie, lecz była w nie zaangażowana zorganizowana grupa przestępcza prowadząca działalność przestępczą w więcej niż jednym państwie;
- zostało popełnione w jednym państwie, lecz powoduje istotne skutki w innym państwie.

Podkreślenia wymaga również fakt, że konwencja z Palermo zobowiązuje państwa-strony do kryminalizacji i penalizacji czterech szczegółowych rodzajów przestępstw, które są zwykle dokonywane w obszarze przestępczości międzynarodowej. Do przestępstw tych należą:

- udział w zorganizowanej grupie przestępczej (art. 5),
- **pranie dochodów z przestępstwa** (art. 6),
- przekupstwo (art. 8),
- czyny przeciwko wymiarowi sprawiedliwości (art. 23).

Kwestię przestępstw transgranicznych oraz zwalczania przestępczości międzynarodowej regulował art. K.1, zawarty w tytule VI Traktatu o Unii Europejskiej z Maastricht z 1992 r.[304], który to zobowiązywał kraje członkowskie do współpracy w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych. Zgodnie z omawianą regulacją dla osiągnięcia celów Unii oraz bez naruszania uprawnień Wspólnoty Europejskiej, państwa członkowskie

[304] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:11992M/TXT [dostęp: 13.05.2019].

obowiązane były traktować określone obszary współpracy jako tematy wspólnego zainteresowania. Wśród wymienionych obszarów wskazać można współpracę policyjną dla celów zwalczania i zapobiegania terroryzmowi, nielegalny handel narkotykami i inne poważne formy przestępczości międzynarodowej, włączając w to – jeśli okaże się to niezbędne ze względu na działanie unijnego systemu wymiany informacji z Europejskim Biurem Policji (tzn. Europolem) – pewne aspekty współpracy celnej. Wymienione zadania miały być realizowane w ramach tzw. trzeciego filaru Unii Europejskiej, początkowo nazwanego „Współpraca w zakresie wymiaru sprawiedliwości i spraw wewnętrznych".

Pewnym przełomem dla zwalczania przestępczości międzynarodowej przez Unię Europejską było podpisanie traktatu amsterdamskiego 2 października 1997 r.[305] Dawny art. K.1 traktatu z Maastricht został w nim znacznie rozszerzony. Nowy art. 29 Traktatu o Unii Europejskiej, zawarty w tytule VI Postanowienia o współpracy policyjnej i sądowej w sprawach karnych, otrzymał następujące brzmienie[306]:

> Bez uszczerbku dla kompetencji Wspólnoty Europejskiej, celem Unii jest zapewnienie obywatelom wysokiego poziomu bezpieczeństwa osobistego w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, przez wspólne działanie Państw Członkowskich w dziedzinie współpracy policyjnej i sądowej w sprawach karnych oraz poprzez zapobieganie i zwalczanie rasizmu i ksenofobii. Cel ten jest osiągany poprzez zapobieganie i zwalczanie przestępczości zorganizowanej lub innej, zwłaszcza terroryzmu, handlu ludźmi i przestępstw przeciwko dzieciom, nielegalnego handlu narkotykami oraz nielegalnego handlu bronią, korupcji i nadużyć finansowych, dzięki:
> – ściślejszej współpracy policji, organów celnych oraz innych właściwych organów w Państwach Członkowskich, prowadzonej zarówno bezpośrednio, jak i za pośrednictwem Europejskiego Urzędu Policji (Europol), zgodnie z postanowieniami artykułów 30 i 32;

[305] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:11997D/TXT [dostęp: 13.05.2019].

[306] K.T. Boratyńska, *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006.

– ściślejszej współpracy organów sądowych oraz innych właściwych organów w Państwach Członkowskich, zgodnie z postanowieniami artykułu 30 litery a)–d) i artykułu 32;
– zbliżaniu, w miarę potrzeby, norm prawa karnego w Państwach Członkowskich, zgodnie z postanowieniami artykułu 31 lit. e).

Przytoczone powyżej przepisy wyposażyły organy Unii Europejskiej w uprawnienie do podejmowania działań w zakresie zwalczania przestępczości międzynarodowej.

Zgodnie z traktatem lizbońskim przepisy dotyczące tego obszaru funkcjonowania przepisów unijnych znalazły swoje miejsce w tytule IV Traktatu o Unii Europejskiej, nazwanym *Przestrzeń wolności, bezpieczeństwa i sprawiedliwości*[307]. Tytuł ten podzielono na następujące jednostki redakcyjne:

Rozdział 1: Postanowienia ogólne,

Rozdział 2: Polityki dotyczące kontroli granicznej, azylu i imigracji,

Rozdział 3: Współpraca sądowa w sprawach cywilnych,

Rozdział 4: Współpraca sądowa w sprawach karnych,

Rozdział 5: Współpraca policyjna.

Szczegółowe uregulowania współpracy pomiędzy członkami Unii w opisywanej sferze zawarto w artykułach od art. 61 do art. 69. Wśród organów wspólnoty zobowiązanych do uczestniczenia w tej współpracy wymienić można Parlament Europejski, Radę oraz Europejskie Jednostki Współpracy Sądowej (tzw. Eurojust).

Kolejnym istotnym aktem prawa unijnego, który należy omówić, jest decyzja Rady Unii Europejskiej z 28 lutego 2002 r. ustanawiająca Eurojust instytucją unijną mającą na celu zwalczanie poważnych przestępstw.

Eurojust można zdefiniować jako wyspecjalizowany organ Unii Europejskiej, którego zadaniem jest umożliwienie pełniejszej współpracy między organami sądowymi państw – członków wspólnoty w zakresie dochodzeń i ścigania przestępstw w przypadku przestępczości międzynarodowej

[307] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=OJ:C:2007:306:TOC [dostęp: 13.05.2019].

i zorganizowanej[308]. Kompetencje Eurojustu wymieniono w art. 4 decyzji Rady z 28 lutego 2002 r. ustanawiającej Eurojust. Są one nastepujące:

Artykuł 4: Uprawnienia

1. Ogólne uprawnienia Eurojustu obejmują:
   a) rodzaje przestępstw, względem których Europol zawsze uprawniony jest do działania na podstawie art. 2 Konwencji o Europolu z dnia 26 lipca 1995 r.:
   b) następujące rodzaje przestępstw:
      - **przestępstwa komputerowe**,
      - **nadużycia finansowe, korupcja oraz wszelkie przestępstwa dotyczące interesów finansowych Wspólnoty Europejskiej**,
      - **pranie brudnych pieniędzy uzyskanych z przestępczości**,
      - przestępstwa przeciwko środowisku naturalnemu,
      - udział w organizacjach przestępczych w rozumieniu wspólnego działania Rady 98/733/WSiSW z dnia 21 grudnia 1998 r. w sprawie uznania za przestępstwo karne udziału w organizacji przestępczej w Państwach Członkowskich Unii Europejskiej;
   c) inne przestępstwa popełniane równocześnie z typami przestępstw określonymi w lit. a) i b).
2. W przypadku przestępstw innego rodzaju, niż te, które są określone w ust. 1, Eurojust może, zgodnie ze swymi celami dodatkowo wspomagać dochodzenie i ściganie na wniosek właściwych władz Państwa Członkowskiego.

   Wspomnieć należy również dyrektywę 2005/60/WE Parlamentu Europejskiego i Rady[309], zgodnie z którą za pranie pieniędzy uznaje się następujące czyny popełnione umyślnie:
   a) konwersję 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 albo udzielenia pomocy osobie, która bierze udział w takiej

[308] A. Grzeszczak, *Unia Europejska wobec przestępczości. Współpraca w ramach III filara*, Kraków 2002.

[309] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32005L0060 [dostęp: 13.05.2019].

działalności, dla umożliwienia jej uniknięcia konsekwencji prawnych takiego działania,

b) ukrycie lub zatajenie prawdziwego charakteru mienia, jego źródła, miejsca położenia, rozporządzania nim, przemieszczania, własności lub praw do mienia, ze świadomością, że mienie to pochodzi z działalności przestępczej lub z udziału w takiej działalności,

c) nabycie, posiadanie lub korzystanie z mienia, ze świadomością w momencie jego otrzymania, że mienie to pochodzi z działalności o charakterze przestępczym lub z udziału w takiej działalności,

d) udział lub współdziałanie w popełnieniu, usiłowanie popełnienia, jak też pomocnictwo, podżeganie, ułatwianie oraz doradzanie przy popełnianiu czynów określonych w powyższych przypadkach. Pranie pieniędzy zachodzi również w przypadku, gdy działania, w ramach których uzyskano mienie mające stać się przedmiotem prania, miały miejsce na terytorium innego Państwa Członkowskiego lub państwa trzeciego.

7.2. Polskie regulacje odnoszące się do omawianych przestępstw

Przestępstwo „prania pieniędzy" reguluje art. 299 k.k.[310] – termin ten nie zostaje jednak wprost użyty. Omawiany przepis w paragrafie pierwszym stanowi:

> § 1. Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, przekazuje lub wywozi za granicę, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

[310] Dz.U. 1997 r. Nr 88, poz. 553.

Paragraf drugi rozszerza zakres omawianego typu czynu zabronionego, dodając, że:

> § 2. Karze określonej w § 1 podlega, kto będąc pracownikiem lub działając w imieniu lub na rzecz banku, instytucji finansowej lub kredytowej lub innego podmiotu, na którym na podstawie przepisów prawa ciąży obowiązek rejestracji transakcji i osób dokonujących transakcji, przyjmuje, wbrew przepisom, środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, dokonuje ich transferu lub konwersji, lub przyjmuje je w innych okolicznościach wzbudzających uzasadnione podejrzenie, że stanowią one przedmiot czynu określonego w § 1 lub świadczy inne usługi mające ukryć ich przestępne pochodzenie lub usługi w zabezpieczeniu przed zajęciem.

Występek finansowania terroryzmu uregulowano w art. 165a k.k., zgodnie z którym:

> § 1. Kto gromadzi, przekazuje lub oferuje środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości w zamiarze sfinansowania przestępstwa o charakterze terrorystycznym lub przestępstwa, o którym mowa w **art. 120** *stosowanie środków masowej zagłady*, **art. 121** *wytwarzanie, gromadzenie i obrót środkami zakazanymi*, **art. 136** *czynna napaść lub znieważenie przedstawiciela obcego państwa*, **art. 166** *piractwo*, **art. 167** *umieszczenie na statku niebezpiecznego urządzenia lub substancji*, **art. 171** *wytwarzanie lub obrót substancjami, materiałami i urządzeniami niebezpiecznymi*, **art. 252** *wzięcie lub przetrzymywanie zakładnika*, **art. 255a** *rozpowszechnianie treści ułatwiających popełnienie przestępstwa o charakterze terrorystycznym* lub **art. 259a** *przekroczenie granicy RP w celu popełnienia na terytorium innego państwa przestępstwa o charakterze terrorystycznym*, podlega karze pozbawienia wolności od lat 2 do 12.
> § 2. Tej samej karze podlega, kto udostępnia mienie określone w § 1 zorganizowanej grupie lub związkowi mającym na celu popełnienie przestępstwa, o którym mowa w tym przepisie, osobie biorącej udział w takiej grupie lub związku lub osobie, która ma zamiar popełnienia takiego przestępstwa.

§ 3. Kto, nie będąc do tego obowiązany na mocy ustawy, pokrywa koszty związane z zaspokojeniem potrzeb lub wykonaniem zobowiązań finansowych grupy, związku lub osoby, o których mowa w § 2, podlega karze pozbawienia wolności do lat 3.
§ 4. Tej samej karze podlega sprawca czynu określonego w § 1 lub 2, który działa nieumyślnie.

Ustawodawca dokonał również wyczerpującego uregulowania kwestii cyberprzestępczości, co obrazuje tabela 7.

Tabela 7. Zestawienie przepisów prawnych dotyczących cyberprzestrzeni.

Akt prawny	Przepis	Charakterystyka
Kodeks karny Rozdział XXXIII Przestępstwa przeciwko ochronie informacji	Art. 265	Nieuprawnione wykorzystanie informacji niejawnych o klauzuli „tajne" lub „ściśle tajne"
	Art. 266	Nieuprawnione ujawnianie lub wykorzystanie informacji w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową
	Art. 267	Uzyskanie dostępu do informacji przeznaczonych dla innych osób, polegające na otwieraniu zamkniętego pisma, podłączaniu się do sieci telekomunikacyjnej lub przełamywaniu albo omijaniu elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń
	Art. 268	Niszczenie, uszkadzanie, usuwanie lub zmiana zapisów istotnej informacji albo w inny sposób udaremnianie lub znaczne utrudnianie osobie uprawnionej zapoznania się z nią
	Art. 268a	Niszczenie, uszkadzanie, usuwanie, zmiana lub utrudnianie dostępu do danych informatycznych albo w istotnym stopniu zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych
	Art. 269	Niszczenie, uszkadzanie, usuwanie lub zmiana danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych. Niszczenie poprzez wymianę informatycznych nośników danych lub przez uszkodzenie urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych
	Art. 269a	Przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej
	Art. 269b	Wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzenia lub programu komputerowego przystosowanego do popełniania przestępstwa, a także hasła komputerowego, kodu dostępu lub innych danych umożliwiających dostęp do informacji, przechowywanych w systemie komputerowym lub sieci teleinformatycznej
Ustawa o zwalczaniu nieuczciwej konkurencji	Art. 23	Ujawnienie innej osobie lub wykorzystanie we własnej działalności gospodarczej informacji stanowiących tajemnicę przedsiębiorstwa uzyskanych w związku z pełnioną funkcją lub uzyskanych bezprawnie

Ustawa o ochronie danych osobowych	Art. 49	Przetwarzanie danych osobowych w zbiorze bez prawa przetwarzania tych danych
	Art. 52	Przy administrowaniu danymi naruszanie choćby nieumyślnie obowiązku zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem
	Art. 53	Niezgłaszanie do rejestracji zbioru danych przez osoby zobowiązane

Źródło: na podstawie ustawy z dnia 6 czerwca 1997 r. Dz.U. Nr 88, poz. 553 z późn. zm.

Znaczenie będzie również mieć ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[311], zgodnie z którą przez pranie pieniędzy rozumie się zamierzone postępowanie polegające na[312]:

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 powyższych sytuacjach również, jeżeli działania, w ramach których uzyskano wartości majątkowe, były prowadzone na terytorium innego państwa niż Rzeczpospolita Polska.

[311] Dz.U. z 2018 r., poz. 723.

[312] M. Capiga, *Bezpieczeństwo instytucji finansowych jako instytucji obowiązanych w systemie przeciwdziałania praniu pieniędzy*, Katowice 2014.

7.3. Charakterystyka przestępstw o charakterze międzynarodowym w instytucjach finansowych popełnianych przez grupy przestępcze

7.3.1. Pranie pieniędzy

Analiza czynu „prania brudnych pieniędzy" nastręcza pewnych trudności z uwagi na fakt, że brak jest jednej, akceptowanej przez wszystkich przedstawicieli doktryny definicji omawianego zjawiska. Można powiedzieć, że jest to *ukrywanie za pomocą różnorodnych działań nielegalnego pochodzenia uzyskanych korzyści, co warunkuje możliwość bezpiecznego (bezkarnego) ich włączenia do legalnego obrotu finansowego i gospodarczego*[313]. Natomiast według innej definicji *pranie pieniędzy to działalność przestępcza mająca na celu legalizację przestępczych dochodów*[314]. Przez pranie brudnych pieniędzy można również rozumieć *dokonywanie w sposób zorganizowany wszelkiego rodzaju działań polegających na nabyciu lub przeniesieniu praw w celu ukrycia dochodów pochodzących z nielegalnych źródeł i wprowadzenia ich do powszechnego obrotu gospodarczego*[315]. W związku z powyższymi rozważaniami możliwe wydaje się stwierdzenie, że cechą definiującą zjawisko brudnych pieniędzy są nielegalne sposoby ich pozyskania, związane najczęściej z handlem bronią, handlem narkotykami, oszustwami finansowymi, działalnością terrorystyczną, nierządem i handlem ludźmi, kradzieżami i łapówkami itd.

Przestępstwo prania pieniędzy jest jednym z najbardziej szkodliwych czynów wymierzonych w interesy gospodarcze państwa, na terenie którego ma miejsce. Przyjmuje się, że do negatywnych następstw należą:

- zakłócenia w systemie podatkowym i walutowym państwa,
- naruszanie zasad uczciwej konkurencji gospodarczej oraz wypaczanie mechanizmu rynkowego określania parametrów ekonomicznych,
- korumpowanie pracowników administracji, decydujących o reglamentacji niektórych sfer działalności gospodarczej,

---

[313] E. Pływaczewski, *Pranie brudnych pieniędzy nowym wyzwaniem dla systemu ekonomiczno-finansowego w Polsce*, [w:] *Proceder prania brudnych pieniędzy. Studia i materiały*, red. *idem*, Toruń 1993.

[314] B. Hołyst, *Kryminalistyka*, Warszawa 2000.

[315] H. Kołecki, R. Jęcz, *Rola i zadania Narodowego Banku Polskiego oraz systemu bankowego w procesie zwalczania procederu prania pieniędzy w Polsce. Podstawowe uwarunkowania i kierunki działań*, [w:] *Proceder prania*…

- przejmowanie niektórych działów gospodarki przez zorganizowane grupy przestępcze,
- wprowadzanie niemoralnych praktyk biznesowych,
- zagrożenie dla prowadzonej przez państwo polityki finansowej poprzez np. utratę wiarygodności międzynarodowej.

Należy podkreślić, że wraz z globalizacją rynku finansowego pranie brudnych pieniędzy coraz częściej nabiera międzynarodowego charakteru. Mechanizm prania pieniędzy w ujęciu transgranicznym sprowadza się do wyprowadzania środków finansowych z systemu finansowego państwa, w którym je pozyskano w sposób sprzeczny z prawem, do systemów krajów, których systemy prawne umożliwią zamaskowanie sposobu ich zdobycia oraz ewentualne ich zalegalizowanie[316]. Na określenie krajów, w których stosunkowo łatwo zrealizować opisaną operację, używa się powszechnie terminu „raj podatkowy". Popełnić omawiane przestępstwo może każda osoba zdolna do ponoszenia odpowiedzialności karnej, także sprawca przestępstwa pierwotnego, w wyniku którego pozyskano nielegalnie środki finansowe. Zaznaczyć jednak należy, że przesłanką, której zaistnienie jest konieczne dla stwierdzenia popełnienia omawianego czynu zabronionego, jest umyślność działania. Chodzi zatem o to, by sprawca miał świadomość popełniania przestępstwa. Generalizując, możliwe jest zdefiniowanie prania brudnych pieniędzy jako wszystkich czynności mających na rzeczywistym celu ukrycie prawdziwego, nielegalnego źródła pochodzenia dochodów[317].

Pogłębiona analiza procesu prania brudnych pieniędzy umożliwia wskazanie trzech kategorii pieniędzy[318]. Jako pierwsze należy wskazać pieniądze czyste. Pod pojęciem tym rozumiemy środki pozyskiwane w związku z legalną działalnością, z której odprowadzono wymagane daniny publiczne. Do drugiej kategorii zaliczyć należy pieniądze szare, czyli uzyskiwane z tzw. szarej strefy, w związku z działalnością prowadzoną bez wymaganego zezwolenia, bez wypełniania obowiązków fiskalnych lub z naruszeniem praw pracowniczych. Do ostatniej kategorii, kluczowej z punktu widzenia niniejszego opracowania, należy zaliczyć pieniądze brudne. Pod pojęciem tym kryją się

[316] J. Grzywacz, *Pranie pieniędzy: metody, raje podatkowe, zwalczanie*, Warszawa 2010.
[317] P. Chodnicka, *Pranie pieniędzy. Regulacje i ryzyko sektora bankowego*, Warszawa 2015.
[318] J.W. Wójcik, *Pranie pieniędzy. Studium prawno-kryminologiczne i kryminalistyczne*, Toruń 1997.

wszystkie pieniądze pochodzące z działalności przestępczej, która w dobie globalnego rynku finansowego przybiera, jak już powiedziano wcześniej, postać międzynarodowej, zorganizowanej działalności.

Należy podkreślić, że pranie brudnych pieniędzy przybiera postać sekwencji zachowań, mających na celu zamaskowanie prawdziwego, nielegalnego źródła pieniędzy oraz nadania im pozorów legalności. Możliwe jest wskazanie głównych metod prania brudnych pieniędzy. Kryterium tego podziału stanowi występowanie stałych i powtarzalnych cech, np. charakterystycznych sposobów przemieszczania środków. Podkreślić jednak należy, że sprawcy zwykle nie są świadomi istnienia konkretnych etapów procesu prania brudnych pieniędzy oraz nazw nadanych im przez doktrynę. Nie w każdej też sytuacji możliwe będzie dokonanie jasnego rozgraniczenia wspomnianych etapów. Zdarzyć się może, że jedna czynność będzie zawierać w sumie naraz elementy dwóch lub więcej faz tego procesu. Dokonując pewnego uproszczenia, możliwe jest wyróżnienie trzech zasadniczych etapów czynności prania brudnych pieniędzy.

Pierwszym z nich jest lokowanie[319] (*placement*), przez które rozumiemy zamianę środków pieniężnych pozyskanych z nielegalnej działalności np. instrumenty finansowe. Proces ten jest możliwy do zrealizowania w drodze tzw. *smurfing*. W ramach tej metody przestępcy korzystają z usług tzw. smerfów, czyli osób, których zadaniem jest otwieranie rachunków w bankach w celu dokonywania na nie wpłat niewielkich sum pieniędzy, co umożliwia uniknięcie mechanizmów kontrolnych, związanych z wartością transakcji. *Smurfing* jako metoda ukrywania pochodzenia pieniędzy jest niezwykle skuteczny, ale również bardzo czasochłonny i pracochłonny. Celem przestępców jest ominięcie progu 15 tys. euro, którego przekroczenie (mowa tu o wartości operacji) zobowiązuje bank do rejestrowania transakcji.

Kolejną metodą prania pieniędzy jest tzw. *blending*. Nazwę tej metody można przetłumaczyć jako mieszanie, a sprowadza się ona właśnie do wymieszania brudnych pieniędzy z dochodami pochodzącymi z legalnego źródła. Zwykle metoda ta jest wykorzystywana w branży o intensywnym i trudnym do oszacowania przepływie gotówki (np. puby, kina, hotele,

[319] R. Lizak, *Pranie pieniędzy w prawie polskim na tle europejskim, międzynarodowym i amerykańskim*, Warszawa 2018.

restauracje). Kolejnym przykładem może być zakup oraz sprzedaż walut obcych w kantorach.

Kolejną metodą prania brudnych pieniędzy, którą należy omówić, będzie tzw. „maskowanie"[320] (*layering*). Proces ten zakłada dokonywanie wielu skomplikowanych transakcji w celu utrudnienia wykrycia rzeczywistego źródła środków finansowych oraz ich rzeczywistego posiadacza w wypadku kontroli. Przykładem czynności realizujących założenia omawianej metody będzie dokonywanie wielu fikcyjnych transakcji, przelewanie na specjalnie w tym celu przygotowane rachunki fikcyjnych osób kwot, których wartość nie będzie przekraczać ustawowych progów oszczędnościowych. Często stosowaną praktyką jest również świadome dokonywanie wadliwych przelewów, na ogół przy wykorzystaniu zagranicznych banków. Wykrycie, wyjaśnienie problemu i zwrot pieniędzy przez bank zajmuje tygodnie, co pozwala przestępcom zyskać na czasie oraz dodatkowo wydłużyć łańcuch transakcji.

Ostatni – proces legitymizacji[321] (*integration*) – sprowadza się do przypisania środkom pochodzącym z nielegalnej działalności legalnych źródeł pochodzenia. Skutecznie przeprowadzona legitymizacja umożliwia swobodne dysponowanie środkami na rynku finansowym. Wśród działań najczęściej podejmowanych w ramach powyższej metody należy wskazać przede wszystkim zawyżanie cen faktur na towary nabyte legalnie (*transfer pricing*), co pozwala osiągnąć zysk równy różnicy pomiędzy ceną realną towaru a zawyżoną ceną na fakturze. Wśród przestępców popularne jest także inwestowanie środków w obrót towarami o trudnej do dokładnego oszacowania wartości (wskazać tu można nieruchomości i luksusowe pojazdy), zaciąganie i spłatę kredytów. Sformułowanie zamkniętego katalogu praktyk stosowanych w tym obszarze wydaje się niemożliwe z uwagi na pomysłowość przestępców. Konkretne praktyki stosowane w celu legitymizacji brudnych pieniędzy dostosowywane są bowiem na bieżąco do zmian prawnych. Według Międzynarodowego Funduszu Walutowego do grupy krajów posądzanych o ułatwianie prania brudnych pieniędzy można zaliczyć Wyspy Bahama, Bahrajn, Kajmany, Hongkong, Antyle, Panama i Singapur[322].

---

[320] *Ibidem.*

[321] *Ibidem.*

[322] Agencja Bezpieczeństwa Wewnętrznego, *Metody prania pieniędzy*, http://www.abw.gov.pl/wolnytekst/69,dok.html [dostęp: 14.05.2019].

Rysunek 4. Fazy prania pieniędzy.

Źródło: opracowanie własne.

Rozwój technologii łączności mający miejsce w ostatnich dekadach przełożył się na rozwój przestępczości finansowej z wykorzystaniem elektronicznych[323]. Możliwość dokonywania transferu pieniędzy na różne rachunki niezależnie od położenia zlecającego oraz bez potrzeby fizycznego kontaktu z pracownikami instytucji finansowej ma ogromną wartość zarówno dla przedstawicieli biznesu, jak i dla międzynarodowych przestępców. Instytucje finansowe oferujące usługi elektroniczne są narażone szczególnie na działalność przestępczą z wykorzystaniem tzw. słupów lub przedsiębiorstw symulujących. Z powyższych względów problem bezpieczeństwa, zwłaszcza bezpieczeństwa systemów informatycznych, ma kluczowe znaczenie dla sprawnej i efektywnej działalności instytucji finansowych. W ustawie o elektronicznych instrumentach płatniczych istnieje zapis zobowiązujący banki działające w oparciu o umowę o usługi bankowości elektronicznej do zapewnienia posiadaczowi konta bezpieczeństwa dokonywania operacji, z zachowaniem należytej staranności oraz przy wykorzystaniu właściwych rozwiązań technicznych. Przeniesienie działań bankowych na platformę globalnej sieci przyniosło jednak całkiem inne rodzaje zagrożeń.

Pojawiły się nowe, nieznane do tej pory metody oszustw i przestępstw charakterystycznych dla internetu (*sniffing*, *tampering*, *spoofing*, *phishing*), który jest siecią otwartą, szczególnie podatną na ingerencję z zewnątrz. Odnotowano także przypadki stosowania internetowych usług płatniczych (*Internet Payment Services*) do realizacji transakcji podejrzanych, polegających na dokonywaniu przy pomocy internetowego systemu płatności znaczącej liczby transakcji, w tym do państw uznawanych powszechnie za tzw. „raje podatkowe".

[323] B. Hołyst, J. Pomykała, *Cyberprzestępczość i ochrona informacji*, Warszawa 2012.

7.3.2. Finansowanie terroryzmu

Finansowanie terroryzmu jest zjawiskiem, które stanowi zazwyczaj przestępstwo zbliżone do prania brudnych pieniędzy. Celem tego procederu jest zazwyczaj ukrycie zarówno wielkości środków zaangażowanych w daną transakcje, jak i tożsamości podmiotów dokonujących transakcji. Rodzaj metody stosowanej w obu przypadkach przez przestępców charakteryzuje się tak znacznym poziomem podobieństwa, iż uprawnione wydaje się mówienie o ich identyczności. Praktyka ustawodawcza zdaje się potwierdzać to założenie, poprzez fakt, że oba zjawiska regulowane są zazwyczaj wspólnie, tak jak np. obecnie w polskim porządku prawnym w jednej kompleksowej ustawie[324]. Z uwagi na zbliżony charakter obu czynów stosuje się do nich zazwyczaj te same przepisy oraz procedury służące ograniczeniu ryzyka wystąpienia niechcianego ryzyka.

Zasadne wydaje się jednak wskazanie, że oba omawiane zjawiska różnią się znacząco co najmniej w jednym ważnym aspekcie. Środki używane do finansowania terroryzmu często nie mogą być zakwalifikowane jako „brudne", tzn. mających źródło w korzyściach pochodzących z popełnienia przestępstwa. Dopiero fakt przeznaczenia środków na finansowanie działań o charakterze terrorystycznym pozwala na stwierdzenie, że dochodzi do złamania prawa. Zauważyć należy, że omawiany czyn stanowi przestępstwo wynikowe i nie wymaga wystąpienia u sprawcy zamiaru.

7.3.3. Cyberprzestępczość

Zjawisko bankowości elektronicznej polega na umożliwianiu przez bank dostępu i zarządu konsumentowi rachunkiem bankowym za pomocą urządzeń elektronicznych takich jak: komputery, smartfony, bankomaty itp.

Wskazać należy, że wraz z wejściem procesu świadczenia usług bankowych w świat cyberprzestrzeni oraz wykorzystaniem sieci internet pojawił się nowy rodzaj zagrożenia bezpieczeństwa banków określany mianem

[324] Ustawa z dnia 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. z 2018, poz. 723.

„cyberprzestępczości”[325]. Powszechnym i dochodowym wśród przestępców zjawiskiem stał się handel różnego rodzaju danymi związanymi z e-bankowością. Przedmiotem przestępstw padają zwykle hasła do kart kredytowych, dane do kont, dane logujące do skrzynek mailowych lub pozwalające na kradzież tożsamości, w różnego rodzaju serwisach internetowych[326].

Jednym z powszechniej występujących sposobów działania wykorzystywanych przez cyberprzestępców są ataki typu *DDos*, *sniffing*, *spoofing*, *phising*, trojany, tzw. metoda „salami” czy *skimming*. Zamieszczona tabela przedstawia dane na temat przestępczości dotykającej sfery bankowej (tabela 8). Szczególnie interesująco prezentuje się zauważalny szybki wzrost stwierdzonych przestępstw popełnianych w związku z e-bankowością.

Tabela 8. Stwierdzone przestępstwa bankowe w latach 2009–2016.

	2009	2010	2011	2012	2013	2014	2015	2016
297 § 1 k.k. (wyłudzenie kredytu)	11 105	11 553	9061	7701	6423	7720	5971	4632
297 § 2 k.k. (niepowiadomienie właściwego podmiotu o sytuacji mogącej mieć wpływ na wstrzymanie albo ograniczenie wysokości udzielonego wsparcia finansowego)	61	73	40	29	46	46	15	11
171 ustawy z 29 sierpnia 1997 r. pr. bank. (prowadzenie działalności bankowej bez zezwolenia)	14	12	10	13	20	12	26	17
304 k.k. (lichwa)	6	57	13	15	21	170	158	40
287 § 1 i 2 k.k. e-bankowość, *phishing*	–	–	–	–	–	527	1027	1615

Źródło: Komenda Główna Policji.

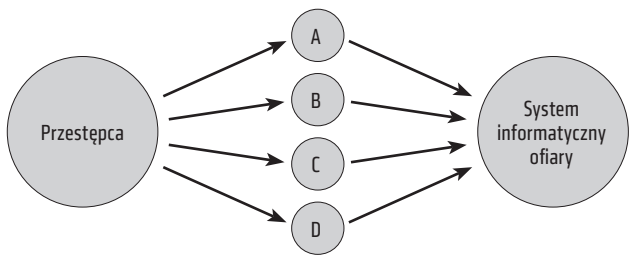
[325] J. Barlińska, A. Małecka, J. Świątkowska, *Cyberbezpieczeństwo. Charakterystyka, mechanizmy i strategie zaradcze w makro i mikro skali*, Warszawa 2018.

[326] Raport Symantec, www.symatec.com [dostęp: 14.05.2019].

7.3.4. Ataki typu DDoS

Distributed Denial of Service (DDoS) to atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (rysunek 5).

Rysunek 5. Schemat ataku DDoS.



Źródło: opracowanie własne.

Atak DDoS stanowi zwykle próbę sparaliżowania dostępu do bankowego serwisu internetowego lub przeprowadzany jest jako próba włamania do systemów komputerowych. Cyberprzestępcy dążą do odwrócenia uwagi administratorów danego systemu informatycznego od bieżącego monitorowania stanu zabezpieczeń, co ma ułatwić wejście w posiadanie wartościowych danych. Dobrym przykładem tego, jak poważne konsekwencje może mieć skutecznie przeprowadzony cyberatak, jest atak na system elektronicznej bankowości Izraela z kwietnia 2013 r., w wyniku którego hakerzy uzyskali dane 30 tys. kart kredytowych.

Omawiany typ ataku sprowadza się do uniemożliwienia dostępu do systemu informatycznego instytucji finansowej. Zgodnie z przewidywaniami cyberprzestępców wewnętrzne jednostki odpowiedzialne za bezpieczeństwo instytucji finansowej są zmuszone do podjęcia działań w celu odblokowania dostępu do systemu. Sprawcy ataku, wykorzystując chwilowe osłabienie kontroli bezpieczeństwa, przejmują wówczas kontrolę nad systemami odpowiedzialnymi za transfer środków pieniężnych[327]. Sprawne wyprowadzenie

[327] T. Hoffman, *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.

środków finansowych instytucji jest możliwe dzięki wcześniejszemu pozyskaniu danych pracownika instytucji, które są potem wykorzystywane do uwierzytelniania transakcji. Dane pracowników pozyskuje się, stosując różnorodne zabiegi socjotechniczne.

W ostatnich latach mamy do czynienia z coraz bardziej wyrafinowanymi metodami przeprowadzania ataków typu DDoS. Przestępcy przed aktywowaniem przejętej sieci urządzeń przeprowadzają analizę systemu informatycznego ofiary oraz dostosowują do nich metodę ataku, co przekłada się na zwiększone straty zaatakowanej instytucji, zwłaszcza jeśli ze względu na typ prowadzonej działalności musi ona zapewniać ciągły dostęp do swoich usług elektronicznych. W przypadku takich podmiotów do strat wynikłych z powodu awarii systemu informatycznego należy jeszcze doliczyć straty związane z utratą wydajności pracy, odzyskiwaniem danych oraz karami finansowymi[328].

W związku z ciągłym rozwojem technologii łączności należy założyć, że ewoluować będą także metody przeprowadzania cyberataków. Ze względu na zmienność metody DDoS konieczna będzie także zmiana podejścia instytucji finansowych do zagrożeń w cyberprzestrzeni. Należy położyć zdecydowany nacisk na większą aktywność wewnętrznych systemów bezpieczeństwa elektronicznego oraz ich zdolność dostosowywania się do zmiennych metod ataku przyjmowanych przez cyberprzestępców.

7.3.5. *Sniffing*

Użytkownicy sieci komputerowych narażeni są szczególnie na przechwytywanie i analizowanie przez przestępców danych przepływających w sieci (tzw. *sniffing*). Wykorzystywane do tego oprogramowanie miało w zamyśle dotyczyć jedynie zadań z zakresu diagnostyki, jednak cyberprzestępcy wykorzystują je przede wszystkim do wykradania danych wrażliwych pozostałych użytkowników sieci. Programy diagnostyczne wykorzystywane w powyższy sposób nie pozostawiają po sobie śladów, przez co wykrycie czynów

[328] P. Wiśniewski, J. Boehlke, *Cyberprzestępczość w gospodarce*, Toruń 2017.

przestępnych popełnianych z ich wykorzystaniem jest znacznie utrudnione[329]. Możliwości, jakie daje oprogramowanie diagnostyczne profesjonalistom, są ogromne. Nie budzi więc zdziwienia fakt, że hakerzy zainspirowani istniejącymi programami postanowili przygotować na ich bazie nowe, jeszcze dokładniejsze narzędzia. Stworzyli oni własne oprogramowanie z myślą o wykradaniu informacji, takich jak numery kart kredytowych i hasła do kont klientów instytucji finansowych korzystających z usług elektronicznych.

Sniffing sam z siebie nie generuje strat u instytucji finansowej – stanowi jednak niezwykle cenne narzędzie dla przestępców. Na przykład numer karty kredytowej zdobyty poprzez podsłuch w sieci może zostać wykorzystany przez osoby nieuprawnione do realizacji płatności.

7.3.6. *Spoofing*

Zjawisko to opiera się na oszukiwaniu ofiary przez przestępców dzięki przyjęciu innej tożsamości. Zazwyczaj da się wyróżnić dwa podstawowe etapy działania przestępców. Po pierwsze, przestępcy podszywają się pod bank. Celem tego działania jest wzbudzenie w ofierze zaufania i wyłudzenie od niej danych wrażliwych, takich jak: numer karty kredytowej, dane osobowe, oraz danych umożliwiających korzystanie z internetowej bankowości. Działanie to ma zazwyczaj na celu skorzystanie z nieuwagi klientów lub wykorzystuje błędy programowe przeglądarek[330].

Działanie przestępne przybiera często formę wysyłania podrobionych wiadomości imitujących korespondencję bankową. Przestępcy zazwyczaj dołączają do wiadomości linki, w których proszą o potwierdzenie tożsamości w formularzu oraz zalogowanie się do fałszywego serwisu. Oczywiście wszystko to jest podstępem mającym na celu wyłudzenie informacji i danych logowania. Próba zalogowania się na podrobionym portalu prowadziła do wycieku danych oraz zdobycia ich przez przestępców. Wykradzione dane pozwalały cyberprzestępcom na podszycie się pod ofiarę, zalogowanie się

[329] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013.
[330] A. Gołębiowska, *Kradzież tożsamości w internecie*, Szczytno 2017.

do serwisu bankowości internetowej oraz ukradzenie środków finansowych umieszczonych na koncie.

Proceder *spoofingu* niezwykle trudno wykryć z uwagi na jego nieinwazyjny charakter. Do samego końca ani ofiara, ani bank mogą się nie orientować, że padli ofiarą przestępstwa. W celu ograniczenia ryzyka *spoofingu* należy podjąć działania zabezpieczające korzystanie z bankowości internetowej. Konieczne wydaje się w tym kontekście używanie zapór sieciowych chroniących prywatność użytkowników. Źródłem zagrożenia może być również korzystanie z niezabezpieczonych i nieznanych sieci bezprzewodowych, dołączenie do których może prowadzić do kradzieży danych.

7.3.7. *Phishing*

Nazwa tego zjawiska pochodzi od angielskiego zwrotu *password harvesting fishing*, czyli łowienia haseł. Proceder ten stanowi jedną z najpowszechniejszych metod działania przestępców w cyberprzestrzeni.

Wydaje się, iż można zaobserwować nasilenie się występowania *phisingu* w ostatnich latach. Jest to najprawdopodobniej związane z upowszechnieniem się bankowości internetowej oraz rutyną, którą wyczuć można w zachowaniach klientów banków, którzy po latach korzystania z udogodnień związanych z dostępem do konta online stają się nieuważni i nieostrożni.

Zazwyczaj elementem tej metody działania przestępców jest podszywanie się pod instytucję, z którą ofiara utrzymuje kontakt. Podobnie jak w wypadku *spoofingu* do oszukiwanego wysyłane są wiadomości mające na celu wyłudzenie wrażliwych danych, takich jak np.: hasła i numery. Najczęściej proszony jest o weryfikacje tożsamości lub logowanie się na konkretnej stronie, która została sfałszowana.

Zjawisko to zdaje się potwierdzać tezę, że najsłabszym ogniwem systemu bezpieczeństwa, w które najłatwiej uderzyć, jest człowiek. Aby ustrzec się przed tego typu oszustwami, należy wykazywać się dużą ostrożnością w komunikacji internetowej oraz pamiętać o fakcie, że bank nigdy nie prosi klientów o przesyłanie swoich danych i haseł w wiadomościach e-mail.

7.3.8. Trojany bankowe

Statystycznie codziennie służby oraz podmioty zajmujące się bezpieczeństwem w sieci znajdują ok. 800 nowych szkodliwych programów, których celem jest kradzież danych oraz haseł do kont bankowych. Jak wskazują w raportach firmy oferujące oprogramowanie antywirusowe, w tym np. Kaspersky Lab, do ich baz dodawanych jest każdego dnia na bieżąco ok. 780 sygnatur nowych szkodliwych programów, które mają za zadanie wydobywać wrażliwe dane. Stanowi to również 1,1% łącznej liczby szkodliwych programów wykrywanych codziennie przez oprogramowanie firmy na komputerach chronionych użytkowników[331].

Wydaje się, że ciekawym przypadkiem ilustrującym omawiane zjawisko może być *Trojan – Banker.MSIL.MultiPhishing.gen*, którego pracownicy Kaspersky Lab skategoryzowali dopiero w styczniu 2012 r. Celem tego złośliwego programu było wyłudzanie kont klientów różnych banków. Ofiarami tego programu padali najczęściej klienci pochodzący z Wielkiej Brytanii[332]. Nie znaczy to oczywiście, że program ten nie był również wykorzystywany przeciwko obywatelom innych krajów. Pamiętać należy, że dzięki powszechności sieci internet, złośliwe oprogramowanie rozprzestrzenia się niezwykle szybko.

Innym ciekawym przypadkiem były odkryte w 2013 r. wersje trojana, *Zeus* zwane *Cytadel* i *Zeus p2p*, których ofiarami padali klienci z Polski. Wirusy tego typu przejmują kontrolę nad komputerem. Zalogowanie się do serwisu bankowego pozwala wirusowi na podszycie się pod system, modyfikację wyświetlanego obrazu lub pojawienie się wiadomości polecających użytkownikom testowe, próbne przelewanie środków itp. Zauważyć należy, że jest to ewidentna próba oszustwa, biorąc pod uwagę powszechną praktykę bankową nieproszenia klientów o dokonywanie operacji finansowych.

CERT Polska poinformowała, że jego eksperci odkryli złośliwe oprogramowanie na system Android, które wymierzone było w polskich klientów banków. Wirus przechwytywał kody jednorazowe potwierdzające transakcje prowadzone na koncie bankowym klienta. Pierwszym etapem oszustwa było zainfekowanie komputera ofiary. Wejście na stronę banku i logowanie

[331] Raport Kaspersky Lab Polska 2012.
[332] http://pclab.pl [dostęp: 14.05.2019].

w serwisie doprowadza do pojawienia się komunikatu konieczności instalacji aplikacji zawierającej „certyfikat E-Security". Zainstalowanie aplikacji na telefonie pozwala przestępcy na uzyskanie dostępu do konta oraz do kodów jednorazowych, pozwalających na dokonywanie przelewów środków pieniężnych.

7.3.9. Metoda salami

Ten rodzaj przestępnej działalności polega na kradzieży niewielkich ilości środków od wielu osób. Kilkaset transakcji jest zmniejszanych o kilkanaście groszy, które są następnie przekazywane na rachunek przestępców i pobierane. Założeniem przyświecającym tego rodzaju działalności jest to, że ofiary tracą na tyle mało środków finansowych, że często nawet tego nie dostrzegają.

7.3.10. *Skimming*

Proceder określany angielskim terminem *skimming* uważany jest obecnie za jeden z najgroźniejszych rodzajów działalności przestępczej związanej z pojawieniem się elektronicznych sposobów płatności, w tym kart płatniczych. Szczególnie wzmożony rozwój przestępczości o tym charakterze nastąpił pod koniec wieku XX.

Nazwa zjawiska pochodzi od angielskiego słowa *skim*, które w tłumaczeniu na język polski oznaczać może słowa takie jak „zabierać" lub „przeglądać"[333].

Skimming w odniesieniu do kart płatniczych przyjmować będzie postać nielegalnego kopiowania pasków magnetycznych zawartych w kartach w celu wytworzenia podróbki, która ma uchodzić za oryginał. Niezwykle trudne jest wykrycie tego procederu z uwagi na fakt, że dane zawarte w pasku mogą być szybko kopiowane w trakcie transakcji kartą w różnych miejscach, takich jak sklepy lub stacje benzynowe. Wytworzenie fałszywej karty pozwala przestępcy na dokonywanie nią transakcji obciążających ofiarę – właściciela oryginału.

[333] J. Fisak, *Słownik współczesny angielsko-polski, polsko-angielski*, Scarborough 2006.

Jedną z najgroźniejszych form, jakie przybrać może *skimming*, jest tzw. *skimming* bankomatowy. W celu zdobycia danych zawartych na karcie płatniczej przestępcy dokonują zazwyczaj modyfikacji samego bankomatu, z którego korzystają klienci. Zazwyczaj modyfikacja polega na zamontowaniu w bankomacie skanera, urządzenia służącego kopiowaniu danych z paska magnetycznego karty. Z uwagi na podobieństwo do oryginalnych rozwiązań technicznych użytych w bankach niezwykle ciężko jest taką bezprawną modyfikację wykryć. Dodatkowo przestępcy umieszczają na bankomacie kamerę mającą za zadanie zarejestrować wpisywaną sekwencję kodu PIN związanego z daną kartą[334].

Zdarza się również, że przestępcy w celu wykradzenia kodu PIN instalują na klawiaturze bankomatu własną nakładkę, która spełniając funkcje klawiatury oryginalnej dodatkowo, zapamiętuje wprowadzony kod.

Do wykradania danych kart służą zazwyczaj małe urządzenia zawierające czytniki oraz zasoby pamięci pozwalające na zapisanie zeskanowanej zawartości. Będąc w posiadaniu danych z zeskanowanych kodów magnetycznych oraz kodów PIN, przestępcy mogą w prosty sposób, korzystając z legalnych urządzeń, takich jak np. kodery kart magnetycznych, podrobić kartę i wykraść środki zawarte na koncie. Wydaje się zasadne ograniczenie powszechności dostępu urządzeń takich jak kodery kart magnetycznych w celu przeciwdziałania przestępczości zorganizowanej wymierzonej w klientów banków.

Wydaje się, że najskuteczniejszym sposobem zwalczania *skimmingu* jest działalność informacyjna skupiona na prewencji oraz edukacji społeczeństwa na temat zagrożeń związanych z używaniem tego rodzaju instrumentów.

7.3.11. *PayPass*

Rozwój technologiczny oraz upowszechnienie się smartfonów doprowadziły do nowego rodzaju działalności przestępczej związanej z możliwością sczytywania za pomocą wgranych na telefony aplikacji danych kart płatniczych. W celu zdobycia danych wymagane jest jedynie krótkie

[334] P. Opitek, *Skimming. Aspekty kryminalistyczne, cyberprzestępczość w bankowości elektronicznej*, Warszawa 2017.

ustawienie telefonu z włączoną odpowiednią aplikacją niedaleko portfela i karty ofiary. Działanie to pozwala na zdobycie danych potrzebnych do dokonania transakcji oraz szybkie jej przeprowadzenie. Ofiara ma możliwość zauważenia niepożądanych operacji na rachunku dopiero po upływie czasu wraz z informacją o historii przepływów finansowych. Z uwagi na ten fakt jest to zjawisko niezwykle trudno wykrywalne, któremu ciężko skutecznie przeciwdziałać. Wydaje się, iż najskuteczniejszą formą walki z tą formą przestępczości jest organizowanie kampanii informacyjnych skierowanych do klientów banków mających na celu podnoszenie świadomości społecznej o zagrożeniach.

7.4. Metody przeciwdziałania przestępczości międzynarodowej w instytucjach finansowych

Wskazane czyny nazywa się, zgodnie z systematyką przyjętą przez Krajowy Nadzór Finansowy[335], mianem oszustw zewnętrznych. Kryterium, na podstawie którego dokonano wyróżnienia tej konkretnej grupy czynów zabronionych, jest brak przynależności podmiotu sprawczego do struktury organizacyjnej instytucji finansowej padającej ofiarą przestępstwa. Zgodnie z polskim prawem oraz przyjętymi standardami dobrych praktyk zarządy instytucji finansowych są zobowiązane do ograniczenia ryzyka przestępczości. Wspomniany obowiązek jest realizowany w ramach procesu zarządzania ryzykiem operacyjnym, poprzez m.in. przygotowanie odpowiednich strategii działania poszczególnych jednostek wewnątrz struktury organizacyjnej instytucji, które utrudnią dokonanie przestępstw na jej szkodę oraz ograniczą ich ewentualne skutki.

Wśród procedur znacząco obniżających ryzyko operacyjne, na które narażone są instytucje finansowe, wskazać można:

- drobiazgową kontrolę czynności dokonywanych z udziałem instytucji finansowej. Szczególną uwagę należy tu położyć na takie cechy, jak

[335] https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_M_8_01_2013_uchwala_8_33017.pdf [dostęp: 14.05.2019].

częstotliwość występowania danych typów operacji oraz ich wartość całkowita,
- zabezpieczenie systemu informatycznego instytucji przed atakiem hakerskim przy pomocy specjalistycznego oprogramowania,
- przeprowadzanie cyklicznych szkoleń dla pracowników instytucji finansowej, które uświadomią im ryzyko oraz wskażą gotowe wzorce zachowań minimalizujących niebezpieczeństwo,
- przeprowadzanie częstych kontroli zarówno przez wewnętrzne jednostki kontrolne, jak i zewnętrznych audytorów.

Do sprawnego wykrywania nieprawidłowości przez pracowników instytucji finansowej konieczne jest posiadanie informacji dotyczących stron transakcji, umożliwiających ich identyfikację. Ustawa o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (dalej: u.o.p.p.p.) obciąża instytucje finansowe szeregiem obowiązków, w tym:
- identyfikacji klienta i weryfikacji jego tożsamości na podstawie dokumentów lub informacji publicznie dostępnych;
- podejmowaniu czynności, z zachowaniem należytej staranności, w celu identyfikacji beneficjenta rzeczywistego i stosowaniu uzależnionych od oceny ryzyka odpowiednich środków weryfikacji jego tożsamości w celu uzyskania przez instytucję obowiązaną danych dotyczących tożsamości beneficjenta rzeczywistego, w tym ustalaniu struktury własności i zależności klienta;
- uzyskiwaniu informacji dotyczących celu i zamierzonego przez klienta charakteru stosunków gospodarczych;
- bieżącym monitorowaniu stosunków gospodarczych z klientem, w tym badaniu przeprowadzanych transakcji w celu zapewnienia, że przeprowadzane transakcje są zgodne z wiedzą instytucji obowiązanej o kliencie i profilu jego działalności oraz z ryzykiem, a także – w miarę możliwości – badaniu źródła pochodzenia wartości majątkowych oraz bieżącym aktualizowaniu posiadanych dokumentów i informacji.

Wszelkie nieprawidłowości mogące świadczyć o istnieniu działalności przestępczej powinny być zgłaszane Krajowemu Inspektorowi Finansowemu, Głównemu Inspektorowi Informacji Finansowych oraz naturalnie organom wymiaru sprawiedliwości.

Zgodnie z polskim prawem daleko posunięta ostrożność i środki bezpieczeństwa powinny być zachowywane w szczególności:

- przy zawieraniu umowy z klientem,
- gdy istnieje podejrzenie prania pieniędzy lub finansowania terroryzmu bez względu na wartość transakcji, formę organizacyjną oraz rodzaj klienta,
- przy przeprowadzaniu transakcji z klientem, z którym instytucja obowiązana nie zawarła uprzednio umowy, której równowartość przekracza 15 000 euro, bez względu na to, czy transakcja jest przeprowadzana jako pojedyncza operacja czy kilka operacji, których okoliczności wskazują, że są one ze sobą powiązane,
- gdy zachodzi wątpliwość, czy otrzymane wcześniej dane identyfikacyjne są prawdziwe lub pełne.

Podstawą działań kontrolnych instytucji finansowej powinno być poznawanie swoich klientów. Ustawa o przeciwdziałaniu praniu pieniędzy nie nakazuje wprost pracownikom instytucji finansowych poznawania klientów, jednak wydaje się, że to właśnie wynika z przytoczonych środków bezpieczeństwa[336]. Należy podkreślić, iż efektywna analiza transakcji dokonywanych przez klientów instytucji wymaga wykorzystania w każdym wypadku całości posiadanej o nich wiedzy. Jako źródło informacji o klientach instytucji finansowej ustawa wskazuje jedynie dokumenty umożliwiające identyfikację stron transakcji, nie oznacza to jednak, że katalog takich źródeł jest zamknięty. Decyzja o tym, na podstawie jakich dokumentów tworzona jest baza danych klientów, zależy zwykle od:

- kosztów pozyskania informacji o klientach,
- trwałości współpracy z klientem,
- profilu klienta (osoba fizyczna, osoba prawna),
- ograniczeń wynikających z ustawy.

Warto zauważyć, że pozyskiwanie informacji o kliencie tylko i wyłącznie z dokumentów przez niego przedstawionych nie ogranicza w znaczący sposób ryzyka. Instytucje finansowe powinny korzystać z innych dokumentów, baz informacji oraz z tzw. otwartych źródeł informacji. Przez otwarte bazy danych należy rozumieć media tradycyjne, fachową literaturę oraz internet.

[336] M. Capiga, *Bezpieczeństwo transakcji finansowych w Polsce*, Warszawa 2015.

7.5. Uwagi *de lege ferenda*

Należy zauważyć, że obecnie głównej trudności w zwalczaniu przestępczości międzynarodowej w sektorze finansowym nie nastręcza karanie sprawców przestępstw – uchwalone w ostatnich latach akty prawa unijnego oraz krajowego wydają się wystarczające do pociągania sprawców czynów do odpowiedzialności. Głównym problemem, z jakim stykają się organy ścigania oraz same instytucje finansowe, jest samo wykrywanie podejrzanych działań odpowiednio wcześnie, co pozwala ograniczyć ryzyko przestępczości finansowej[337].

Przestępczość finansowa ma charakter sytuacyjny, przestępcy finansowi poszukują luk w zabezpieczeniach instytucji i dopiero po ich znalezieniu podejmują ostateczną decyzję o dokonaniu przestępstwa. Przyjęcie odpowiednich metod zarządzania ryzykiem przez instytucje finansowe stanowi z tego powodu najskuteczniejszą metodę przeciwdziałania przestępczości finansowej w instytucjach finansowych.

Możliwe wydaje się jednak wyróżnienie najważniejszych procedur i metod umożliwiających znaczne ograniczenie ryzyka oszustw w instytucjach finansowych. Na podstawie badań przeprowadzonych przez Międzynarodowe Stowarzyszenie Audytorów (*Association of Certified Fraud Examiners*, dalej: ACFE) można wskazać:

- bieżącą analizę danych dokonywanych operacji – możliwą dzięki zapewnieniu sprawnego przepływu i gromadzeniu informacji pozwalających oceniać rzeczywiste przepływy środków w ramach operacji dokonywanych z udziałem instytucji finansowej,
- częste kontrole wykonywane przez zarząd instytucji finansowej – zarząd, posiadający dostęp do wszystkich informacji związanych z operacjami instytucji, powinien na bieżąco kontrolować działania pracowników,
- utworzenie tzw. gorącej linii wewnątrz struktury organizacyjnej instytucji – wytworzenie odpowiednich kanałów komunikacyjnych umożliwiających szybkie, anonimowe informowanie o nieprawidłowościach mających miejsce w instytucji nie tylko zachęci pracowników oraz klientów do informowania o takowych, ale także umożliwi szybszą

[337] M. Capiga, *Ocena bezpieczeństwa funkcjonowania instytucji finansowych*, Warszawa 2013.

reakcję odpowiednich organów instytucji, ograniczając czas trwania oszustwa i poniesione straty,

- obowiązek przekazania sprawozdań finansowych zarządowi do akceptacji – członkowie zarządu powinni mieć rzeczywisty wgląd w całościową sytuację finansową instytucji, co powinno się przełożyć na szybsze reagowanie na ewentualne nieprawidłowości,
- niezapowiedziane audyty – utrudniają ukrywanie przez przestępców śladów pozostałych po dokonanych przez nich ingerencjach w system instytucji finansowej oraz przełożą się na większą czujność pracowników,
- wyodrębnienie wewnątrz struktury organizacyjnej instytucji jednostki odpowiedzialnej za monitorowanie oraz przeciwdziałanie ryzyku przestępczości finansowej – wykwalifikowani pracownicy, świadomi najnowszych zagrożeń związanych z przestępczością finansową są jednym z ważniejszych czynników pozwalających na szybkie i skuteczne przeciwdziałanie nieautoryzowanym ingerencjom w system instytucji finansowej,
- szkolenie kadry menedżerów i kierowników dotyczące oszustw finansowych – kontrola ryzyka winna być sprawowana na wszystkich szczeblach organizacyjnych instytucji finansowej,
- szkolenie pracowników dotyczące oszustw finansowych – informacje przekazywane przez pracowników instytucji finansowych na temat luk w zabezpieczeniach instytucji oraz dostrzeżonych nieprawidłowości stanowią najczęstszą przyczynę wczesnego wykrywania oszustw finansowych. Przeprowadzanie cyklicznych szkoleń pracowników instytucji dotyczących najnowszych zagrożeń bezpieczeństwa jest w konsekwencji najważniejszą metodą zapobiegania przestępczości finansowej, w tym przestępczości finansowej,
- przygotowanie przez instytucję finansową zabezpieczeń wewnętrznego systemu informatycznego dostosowanych do poziomu ryzyka, na jakie narażona pozostaje instytucja. Ocena ryzyka powinna być na bieżąco aktualizowana w ramach procedur wypracowanych przez zarząd w procesie zarządzania ryzykiem.

Zgodnie z badaniami ACFE[338] zgłoszenie nieprawidłowości przez pracowników instytucji finansowej pozwala na wczesne wykrycie oszustwa w około 25% przypadków, stąd jest sprawą najwyższej wagi z punktu widzenia instytucji finansowej, by utrzymywać wśród pracowników wysoki poziom kultury etycznej opartej na szczerości. Równie ważne jest w związku z powyższym ciągłe podnoszenie kwalifikacji pracowników umożliwiające im rozpoznawanie i trafną ocenę współczesnych zagrożeń. W poniższej tabeli porównano średnie straty instytucji finansowych stosujących omawiane metody ograniczania ryzyka przestępczości finansowej w 2018 r. (tabela 9).

Tabela 8. Średnie straty instytucji finansowych stosujących metody ograniczania ryzyka przestępczości finansowej w 2018 roku.

Środek służący ograniczeniu ryzyka	Odsetek badanych spraw, w których dany środek był stosowany	Straty mimo zastosowania danego środka	Straty w wypadku niestosowania danego środka	Redukcja strat podana w procentach
Ustalenie zasad postępowania pracowników	80%	$110 000	$250 000	56%
Bieżąca kontrola danych dotyczących operacji danej instytucji	37%	$80 000	$165 000	52%
Niezapowiedziany audyt	37%	$75 000	$152 000	51%
Audyt zewnętrzny	67%	$100 000	$200 000	50%
Przegląd na poziomie kierownictwa danej instytucji	66%	$100 000	$200 000	50%
Utworzenie tzw. „gorącej linii"	63%	$100 000	$200 000	50%
Polityka odnośnie do postępowania na wypadek oszustw	54%	$100 000	$190 000	47%
Jednostka audytu zewnętrznego	73%	$108 000	$200 000	46%
Zatwierdzanie sprawozdań finansowych przez radę nadzorczą	72%	$109 000	$192 000	43%
Szkolenia pracownicze w zakresie postępowania na wypadek oszustwa	53%	$100 000	$169 000	41%
Wprowadzenie procedur oceny ryzyka oszustwa	41%	$100 000	$162 000	38%

[338] *Report to the Nations. 2018 Global Study on Occupational Fraud and Abuse*, Association of Certified Fraud Examiners.

Środek służący ograniczeniu ryzyka	Odsetek badanych spraw, w których dany środek był stosowany	Straty mimo zastosowania danego środka	Straty w wypadku niestosowania danego środka	Redukcja strat podana w procentach
Programy wsparcia dla pracowników	54%	$100 000	$160 000	38%
Szkolenia z postępowania na wypadek oszustw dla osób zajmujących stanowiska kierownicze	52%	$100 000	$153 000	35%
Wydzielenie jednostki organizacyjnej odpowiedzialnej za zarządzanie ryzykiem oszustwa	41%	$100 000	$150 000	33%
Zewnętrzna kontrola sprawozdań finansowych	80%	$120 000	$170 000	29%
Rotacja pracowników	19%	$100 000	$130 000	23%
Uniezależnienie jednostek audytu	61%	$120 000	$150 000	20%
Program nagród dla sygnalistów	12%	$110 000	$125 000	12%

Źródło: Opracowanie na podstawie: *Report to the Nations on Occupational Fraud and Abuse 2018 Global Fraud Study, Association of Certified Fraud Examiners*

Na podstawie badań przeprowadzonych przez ACFE na międzynarodowym rynku finansowym można stwierdzić, że już samo wprowadzenie procedur, takich jak: bieżąca analiza operacji, niezapowiedziane audyty, kontrole przeprowadzane regularnie przez zarząd instytucji czy istnienie specjalnej gorącej linii do raportowania nieprawidłowości, powinny umożliwić redukcję ryzyka oszustwa na poziomie 50%.

Podkreślenia wymaga fakt, że nie jest możliwe całkowite zlikwidowanie ryzyka przestępczości finansowej, w tym przestępczości międzynarodowej, które dotyka instytucji finansowych. Możliwe jest jednak jego znaczące ograniczenie, jednak pod warunkiem, że zarząd instytucji sumiennie wywiązuje się ze swoich obowiązków przygotowywania odpowiednich procedur zarządzania ryzykiem.

ROZDZIAŁ ÓSMY

Analiza i metody zapobiegania przestępstwom finansowym dokonywanym przez klientów instytucji finansowych

Jedno z najgroźniejszych zjawisk, z jakimi zmuszone jest radzić sobie państwo, stanowi przestępczość gospodarcza. Dzieje się tak z uwagi na fakt, że jest to jedno ze źródeł najwyższych strat, zarówno dla budżetu, jak i podmiotów prywatnych[339]. Duży wpływ na rozwój form przestępczości oraz charakter i natężenie zjawiska szarej strefy ma kształt przyjętej przez państwo polityki podatkowej oraz skuteczność jej realizacji. Zjawisko przestępczości podlega więc szczególnej analizie nie tylko ze względu na bezpieczeństwo publiczne, ale również ze względu na bezpieczeństwo gospodarczego kraju. Poziom przestępczości w sposób bezpośredni przekłada się na opłacalność i sposób prowadzenia działalności gospodarczej. Częstym zjawiskiem towarzyszącym nieprawidłowościom gospodarczym jest typowa przestępczość kryminalna, np. fałszerstwa, pranie pieniędzy oraz korupcja. Polski model zapobiegania przestępczości gospodarczej przewiduje istnienie i działanie obok siebie wielu służb, organów oraz instytucji w przypisanych im sferach gospodarki. Zauważyć więc należy, że model ten zakwalifikować można jako charakteryzujący się rozproszoną ochroną[340].

Przestępczość gospodarcza ma różnorodny charakter. Za typowo występujące zjawisko uznać można przestępczość podatkową, najczęściej przejawiającą się w postaci unikania płacenia podatków oraz wyłudzania nienależnych zwrotów, a także zaniżania należności publicznoprawnych. Ponadto zalicza się do niej również przestępczość związaną z zamówieniami publicznymi

[339] *Program przeciwdziałania i zwalczania przestępczości gospodarczej na lata 2015–2020.*

[340] P. Łabuz, I. Malinowska, M. Michalski, T. Safjański, *Przestępczość gospodarcza. Istota zjawiska. Zasady odpowiedzialności, mechanizmy przestępcze i metody działania sprawców*, Warszawa 2017.

czy przeciwko prawom autorskim i pokrewnym, a także wszystkie rodzaje przestępczości ukierunkowanej na uzyskiwanie zysku przy uwzględnieniu mechanizmów rynkowych. Charakterystyczną odmianą przestępczości gospodarczej jest przestępczość występująca w ramach rynku kapitałowego, bankowego i ubezpieczeniowego. Z uwagi na zwyczajową sprawność przestępców gospodarczych w dostosowywaniu metod działania do zmieniającej się sytuacji ekonomicznej oraz przepisów prawa krajowego i wspólnotowego, przestępczość gospodarcza jest najszybciej ewoluującym rodzajem działalności przestępczej[341].

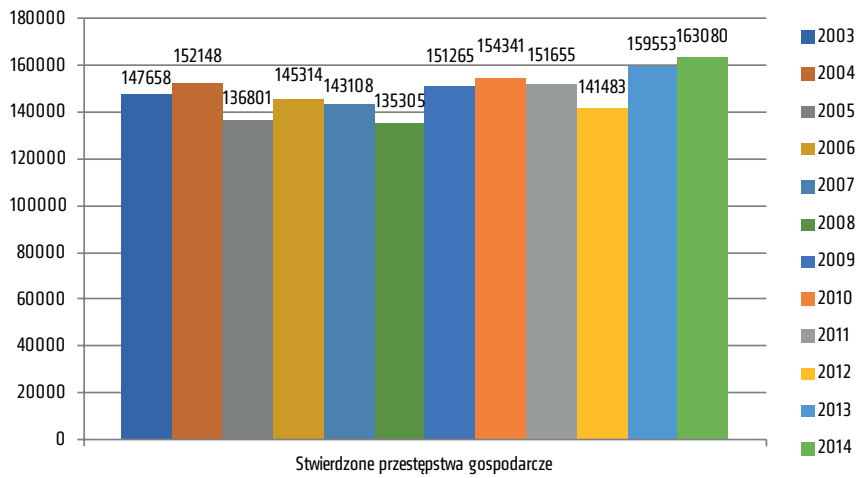
Podstawową trudnością towarzyszącą zapobieganiu przestępczości gospodarczej jest fakt częstego powiązania i współfunkcjonowania działalności przestępczej oraz legalnej działalności gospodarczej. Zjawisko to w znacznym stopniu utrudnia zbadanie wielkości oraz charakteru udziału konkretnych osób działalności niezgodnej z prawem oraz określenie wielkości omawianego zjawiska. Nierzadko dochodzi również do nieświadomego wykorzystania właścicieli oraz ich legalnie działających firm w przedsięwzięciach niezgodnych z prawem. Równie często dochodzi do wykorzystywania legalnie działających podmiotów gospodarczych w przestępczej działalności. Podkreślić należy także, że z uwagi na informatyzację systemu finansowego, coraz powszechniejsze stają się tzw. cyberprzestępstwa. Pomysłowi przestępcy wykorzystują powszechnie zdobycze technologiczne takie, jak powszechny dostęp do internetu, do prowadzenia działalności przestępczej przy zachowaniu anonimowości, z pominięciem granic państw. Należy jednak zauważyć, że dostęp do cyberprzestrzeni dostarcza jedynie nowych środków prowadzenia przestępczej działalności lub stanowi nową przestrzeń, w której taka działalność jest prowadzona, nie tworzy zatem zupełnie nowych typów czynów zabronionych. Za dobry przykład mogą posłużyć oszustwa internetowe, w tym oszustwa dokonywane przy pomocy internetowych serwisów aukcyjnych, nielegalny handel towarami akcyzowymi, nielegalny hazard oraz przestępstwa na szkodę właścicieli dóbr intelektualnych. Na marginesie należy wskazać, że przestępczość gospodarcza jest ściśle powiązana z tzw. praniem brudnych

[341] L. Wilk, *Przestępczość gospodarcza – pojęcie, przyczyny, sprawcy*, „Edukacja Prawnicza" 2012, nr 10.

pieniędzy, czyli na ukrywaniu przestępczego pochodzenia określonych składników majątkowych, co samo w sobie stanowi przestępstwo[342].

Zgodnie z danymi Policji z 2003–2014 liczba stwierdzonych przestępstw gospodarczych utrzymuje się na stałym poziomie i w skali roku oscyluje wokół 150 000, przy czym w 2014 roku odnotowano najwyższą liczbę stwierdzonych przestępstw gospodarczych w analizowanym okresie, tj. 163 080.

Wykres 1. Liczbę stwierdzonych przez Policję przestępstw gospodarczych w latach 2003–2014[343].

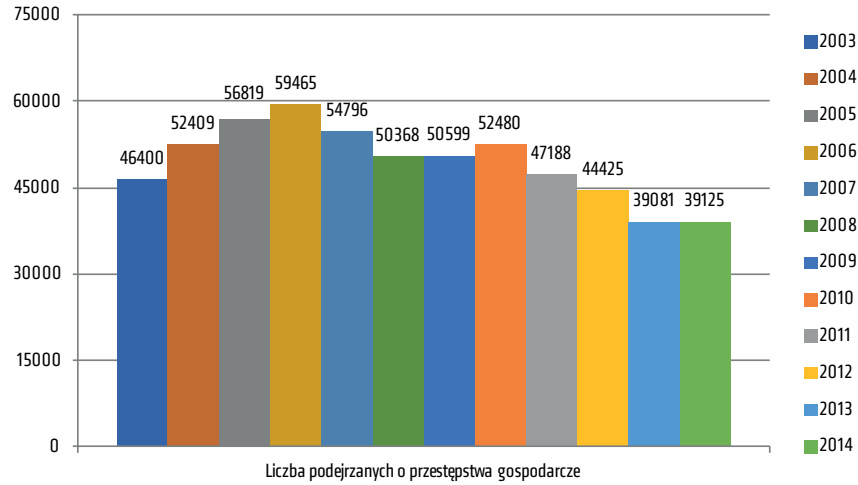


Podkreślenia wymaga jednak fakt, że od 2009 roku sukcesywnie spada liczba podejrzanych o popełnienie przestępstwa gospodarczego.

[342] N. Ciszewska, *Przestępstwa gospodarcze – istota i rodzaje*, „Studia nad Bezpieczeństwem" 2016, nr 1.

[343] *Program przeciwdziałania i zwalczania…*

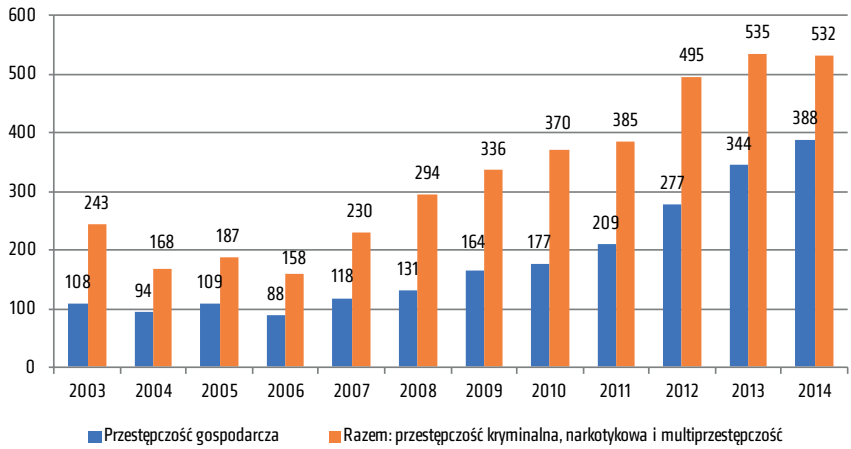
Wykres 2. Liczba osób podejrzanych o przestępstwa gospodarcze na podstawie danych Policji w latach 2003–2014.



Wskazać należy, że spadek liczby osób podejrzanych w powiązaniu ze wzrostem stwierdzonych przestępstw świadczy o popełnianiu coraz bardziej złożonych (składających się z wielu czynów zabronionych) przestępstw gospodarczych, niewątpliwie także w ramach zorganizowanych grup przestępczych.

Wniosek ten zdaje się potwierdzać fakt wzrostu liczby zorganizowanych grup przestępczych, które pozostają w zakresie zainteresowania Centralnego Biura Śledczego Policji. Od 2011 r. wzrost ten dotyczy w szczególności liczby grup przestępczych o charakterze gospodarczym.

Wykres 3. Liczba zorganizowanych grup przestępczych działających w obszarze przestępczości gospodarczej, względem liczby pozostałych zorganizowanych grup przestępczych, które pozostają w zakresie zainteresowania CBŚP w latach 2003–2014.



Należy zauważyć, że to właśnie w sprawach dotyczących przestępczości gospodarczej wykorzystuje się najczęściej procedury zabezpieczenia mienia i dalszego jego odzyskania. Wyjaśnieniem tego trendu zdaje się okoliczność, że ta właśnie kategoria przestępstw ma za przedmiot największe wartości majątkowe.

8.1. Przestępczość na rynku bankowym

Do najbardziej typowych przestępstw występujących na rynku bankowym należą: fałszerstwa, przedkładania podrobionego, przerobionego, poświadczającego nieprawdę albo nierzetelnie wypełnianego dokumentu bądź pisemnego oświadczenia o istotnym znaczeniu, w celu uzyskania kredytu, pożyczki pieniężnej, poręczenia, gwarancji, akredytywy, dotacji, subwencji, potwierdzenia zobowiązania wynikającego z poręczenia lub z gwarancji lub podobnego świadczenia pieniężnego na określony cel gospodarczy, elektronicznego

instrumentu płatniczego lub zamówienia publicznego. Najczęściej sprawcami tego rodzaju przestępstw są sami klienci banków[344].

Za charakterystyczne dla tego rodzaju przestępczości uznać należy również sytuacje niewywiązywania się z obowiązku powiadamiania właściwego podmiotu o powstaniu sytuacji mogącej potencjalnie ograniczyć wysokości udzielonego wsparcia finansowego lub zamówienia publicznego bądź też dalszego korzystania z elektronicznego instrumentu płatniczego.

Przestępstwa tego rodzaju skierowane najczęściej bywają w stronę banków, podobnych jednostek organizacyjnych, a także organów i instytucji dysponujących środkami publicznymi.

Zjawiskiem korzystnym dla przestępców działających na rynku bankowym są błędne decyzje o przyznaniu kredytów osobom fizycznym i podmiotom gospodarczym, poprzedzone zazwyczaj[345]:

- kierowaniem wniosków kredytowych przez osoby posługujące się sfałszowanymi dokumentami. Proceder bywa również zazwyczaj połączony z uzyskiwaniem zezwolenia na prowadzenie działalności gospodarczej i numeru REGON stanowiącego podstawę do otwierania rachunku bankowego dla fikcyjnego klienta;
- kierowaniem wniosków kredytowych przez podmioty niespełniające wymagań do udzielenia kredytu;
- fałszowaniem dokumentów potwierdzających zdolność kredytową firmy;
- ukrywaniem zadłużenia firmy;
- podawaniem nieprawdziwych informacji dotyczących przedmiotu będącego prawnym zabezpieczeniem kredytu;
- przedstawianiem niewiarygodnych poręczycieli, którym w przeszłości zarzucano posługiwanie się fałszywymi dokumentami, poręczających kilka kredytów pobieranych przez jednego lub kilku kredytobiorców;
- wzajemnym poręczaniem kredytów.

Wyłudzenia i oszustwa na rynku bankowym występują również jako próby wykradania środków gromadzonych na rachunkach bankowych

[344] W. Jaroch, *Zagrożenia systemu bankowego jako kategoria przestępczości gospodarczej. Zagrożenia w sektorze bankowym. Analiza kryminalna zjawisk oraz możliwości przeciwdziałania*, Olsztyn 2013.

[345] *Ibidem.*

z wykorzystaniem skradzionych bądź podrobionych dowodów osobistych oraz jako próby zakładania przedsiębiorstw oraz kont bankowych z wykorzystaniem osób ubezwłasnowolnionych[346]. Dynamicznie rozwijająca się technologia oraz ewolucja sposobów świadczenia usług na rynku bankowym sprawia, że klienci narażeni są na różne nowe zagrożenia, w tym włamanie do zasobów informatycznych banku, *phishing* oraz *skimming*. W przypadku złamania zabezpieczeń systemu informatycznego banku zagrożenie dotyczy głównie ryzyka utraty poufności danych oraz szkód wizerunkowych. Zagrożenia utraty danych oraz włamań do systemu bankowego możemy podzielić na zagrożenia wewnętrzne – zasadniczo groźniejsze, bo wykonywane zazwyczaj przez pracowników banków, oraz zewnętrzne, wykonywane przez osoby spoza banku, zwykle poprzez sieć internet[347].

W przypadku *phishingu*, który polega na pozyskiwaniu za pośrednictwem internetu wrażliwych danych – haseł ID, loginów, itp., umożliwiających przestępcze dokonywanie operacji finansowych drogą elektroniczną, na kontach bankowych, bez wiedzy i zgody ich prawowitych właścicieli, można ataki podzielić na: profilowane, których celem jest konkretna osoba albo grupa osób oraz masowe, skierowane do szerokiej grupy podmiotów. Skuteczność tych ataków jest niższa niż w przypadku ataków profilowanych, a stosowanie przez banki rozwiązania w postaci haseł jednorazowych, blokad konta przy niewielkiej liczbie prób błędnego logowania oraz podstawowych zasad bezpieczeństwa przez klientów banku wydaje się wystarczać do ograniczenia tego typu zagrożeń.

Skimming oznacza nielegalne kopiowanie zawartości paska magnetycznego bez wiedzy jej posiadacza w celu wytworzenia kopii i wykonywania płatności za towary i usługi oraz płatności z bankomatów. Zwykle dochodzi do tego poprzez niedozwolone modyfikowanie bankomatów oraz instalowanie w nich odpowiednich urządzeń.

---

346 *Ibidem.*

347 A. Lewkowicz, *Sektor bankowy z perspektywy cyberprzestępczości. Zagrożenia w sektorze bankowym. Analiza kryminalna zjawisk oraz możliwości przeciwdziałania*, Olsztyn 2013.

8.2. Przestępczość na rynku ubezpieczeń

Najczęstszymi sprawcami przestępstw na rynku ubezpieczeń są klienci dążący do uzyskania nienależnych im środków pieniężnych[348]. Pojęcie „przestępczości ubezpieczeniowej" obejmuje wszelkie działania lub zaniechania zmierzające do uzyskania nienależnego odszkodowania oraz skierowane przeciwko zakładom ubezpieczeń lub instytucjom ubezpieczeniowym. Przestępczość ta stanowi poważną przeszkodę w funkcjonowaniu rynku ubezpieczeń, a jej skutki ponoszą zarówno zakłady ubezpieczeń (np. straty finansowe), jak i ich klienci (np. wyższe składki, upadłości firm ubezpieczeniowych). Powszechnymi mechanizmami dokonywania przestępstw na rynku ubezpieczeń są[349]:

- pozorowanie kolizji drogowych mające na celu wyłudzenie świadczeń bądź odszkodowań;
- tworzenie pozoru kradzieży samochodów, w tym stanowiących własność banków i firm leasingowych (jak w przypadku zagrożenia spłaty kredytu na skutek gorszej sytuacji finansowej kredytobiorcy);
- próby wyłudzania odszkodowań w związku z umyślnie powodowanymi pożarami;
- wyłudzenia świadczeń z tytułu zawartych umów ubezpieczeń wypadkowych lub ubezpieczeń na życie, na podstawie upozorowanych bądź zaaranżowanych zdarzeń, objętych ochroną ubezpieczeniową (celowe uszkodzenia ciała, fałszywe akty zgonu);
- pobieranie odszkodowań z kilku zakładów ubezpieczeń za tę samą szkodę;
- zawyżanie kosztów napraw poprzez wykorzystywanie fałszywych bądź poświadczających nieprawdę rachunków z zakładów naprawczych,
- zawyżanie wartości ubezpieczonych obiektów (nieruchomości, samochodów i innych dóbr ruchomych) i poświadczanie nieprawdy przez agentów celem umożliwienia uzyskania kredytu oraz większego odszkodowania;

[348] R. Połeć, M. Lemańczyk, *Przeciwdziałanie przestępczości ubezpieczeniowej w aspekcie jej społecznej akceptacji*, „Studia Oeconomica Posnaniensia" 2015, nr 11.

[349] J. Talarek, *Przestępczość w Polsce na tle wybranych krajów*, „Prawo. Ubezpieczenia. Reasekuracja" 2004, nr 2.

- wyłudzanie gwarancji ubezpieczeniowej zapłaty wierzytelności handlowych.

Wyłudzenia z tytułu ubezpieczenia działalności gospodarczej, ryzyk finansowych i ubezpieczeń osobowych często występują w powiązaniu z założeniem lub przejęciem przez przestępców działalności gospodarczej. Opanowany podmiot gospodarczy służy dokonywaniu wyłudzeń z tytułu ubezpieczeń komunikacyjnych, ubezpieczeń gospodarczych i ryzyk finansowych, ubezpieczeń mienia od ognia i kradzieży oraz ubezpieczeń osobowych. Na chwilę obecną największą bolączką systemu ubezpieczeń jest wzrost zainteresowania i większa aktywność zorganizowanych grup przestępczych, specjalizujących się w przestępczości ubezpieczeniowej. Grupy korzystają z wypróbowanych metod wyłudzania świadczeń, a także nastawiają się na jednoczesne działanie w wielu zakładach ubezpieczeń, co przekłada się na wielość podmiotów poszkodowanych w wyniku przestępstw. Warto również podkreślić w tym miejscu, że grupy przestępcze rzadko ograniczają się do działalności na jednym tylko rynku. Przykładowo część przestępców ubezpieczeniowych działa jednocześnie na rynku bankowym.

8.3. Przestępczość na rynku kapitałowym

Przestępcy działający w sferze gospodarczej podejmują się również takich prób na rynku kapitałowym. Do nieprawidłowości dochodzi podczas obrotów instrumentami finansowymi na rynkach Giełdy Papierów Wartościowych w Warszawie S.A.[350] oraz w szeroko rozumianych procesach inwestycyjnych związanych z funduszami inwestycyjnymi lub ubezpieczeniowymi, obligacjami rządowymi, samorządowymi lub korporacyjnymi. Najczęstszymi formami przestępstw na rynku kapitałowym są:

- prowadzenie działalności w zakresie obrotu instrumentami finansowymi bez zezwolenia Komisji Nadzoru Finansowego. Działalność ta polega zazwyczaj na wykonywaniu czynności maklerskich, przyjmowaniu

[350] M.S. Niedużak, *Badanie występowania transakcji z wykorzystaniem informacji poufnych na Giełdzie Papierów Wartościowych w Warszawie*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2013, nr 904.

i przekazywaniu zleceń, zarządzaniu portfelami, doradztwie inwestycyjnym lub organizowaniu alternatywnego systemu obrotu;
- fałszowanie danych w dokumentach informacyjnych lub zatajanie prawdziwych danych;
- oferowanie papierów wartościowych bez wymaganego ustawą zatwierdzenia prospektu emisyjnego lub memorandum informacyjnego, polegające na publikacji ogłoszeń o zamiarze zbycia instrumentów finansowych w mediach;
- ujawnienie i wykorzystanie informacji poufnej[351];
- manipulacyjne operacje o charakterze spekulacyjnym.

Dzięki rozwojowi technologicznemu oraz pojawieniu się nowych narzędzi, takich jak np. internet, przestępcom o wiele łatwiej jest zachować anonimowość oraz utrudnić wykrycie przestępstwa. Szczególnie niebezpieczne pod tym kątem wydają się podmioty oferujące usługi zarządzania środkami, które – działając bez zezwolenia – pozyskują klientów obietnicą znaczących zysków.

8.4. Pranie pieniędzy z przestępstw

Proceder prania pieniędzy służy ukrywaniu prawdziwych i nielegalnych źródeł pochodzenia dóbr uzyskanych za pomocą niezgodnej z prawem działalności. Jest to jeden z najbardziej typowych i charakterystycznych rodzajów przestępczości gospodarczej. Z uwagi na charakter oraz skomplikowanie procesów gospodarczych to właśnie w tej sferze zaobserwować można najbardziej złożone metody prania pieniędzy. Dzieje się tak z uwagi na fakt, że ich sprawcy dysponują zwykle profesjonalną wiedzą na temat złożonych mechanizmów finansowych, a proces prania pieniędzy jest nierzadko wpisany w schemat samego przestępstwa gospodarczego będącego pierwotnym[352]. Przestępstwem pierwotnym bywa każde przestępstwo przynoszące przestępcy konkretną korzyść majątkową. Do najczęściej stwierdzanych przestępstw

[351] Cz. Martysz, *Prawne i ekonomiczne aspekty karalności insider tradingu*, Warszawa 2013.

[352] J. Sawicka, E. Marcinkowska, A. Stronczek, *Ujawnienie przestępstw prania pieniędzy przez pracowników zawodów księgowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach", 2017, nr 34.

bazowych należą przestępstwa związane z wyłudzeniami VAT[353]. Przestępcy najczęściej działają w branżach oraz dziedzinach takich jak: obrot wyrobami elektronicznymi, komponentami biopaliw i metalami szlachetnymi. Do prania pieniędzy wykorzystywane są różnorodne instrumenty gospodarcze. Dużym zagrożeniem utrudniającym wykrycie przestępstwa oraz zlokalizowanie nielegalnych dóbr jest proceder mieszania środków finansowych pochodzących z legalnej działalności ze środkami pochodzącymi z działalności przestępczej. Operacji takich dokonuje się najczęściej poprzez usługi świadczone przez instytucje, takie jak: banki, domy maklerskie, towarzystwa funduszy inwestycyjnych, kantory, itd. Dotyczy to również transakcji na rynku nieruchomości, transakcji obrotu surowcami wtórnymi, usług oferowanych przez restauracje, salony gier itd., prowadzonych z wykorzystaniem uproszczonych form opodatkowania.

Kolejne ze zjawisk godzące bezpośrednio w bezpieczeństwo budżetowe państwa polega na dokonywaniu fikcyjnych transakcji. Rynkami szczególnie narażonymi w związku z tego rodzaju działalnością przestępczą są rynek paliw płynnych i gazowych, obrót złomem i metalami kolorowymi oraz różnego rodzaju usługi, w ramach których możliwe jest przeprowadzanie trudnych do wykrycia fikcyjnych transakcji. Częstym i stwarzającym dodatkowe trudności elementem procederu prania pieniędzy jest międzynarodowy charakter działalności[354]. Transakcje finansowe z podmiotami posiadającymi siedzibę lub rachunki w innych krajach wykorzystywane są do przerywania możliwości śledzenia łańcucha transakcji przez powołane do tego instytucje państwowe. Wymusza to współpracę oraz koordynację działań służb oraz organów podatkowych z ich odpowiednikami w innych krajach dla zapewniania właściwych rozwiązań w zakresie współpracy międzynarodowej w celu przeciwdziałania zjawisku prania pieniędzy, w szczególności w zakresie efektywnej wymiany informacji i stosowania ustalonych standardów. Kolejną trudność stanowi fakt, że procederowi prania pieniędzy sprzyjają procesy globalizacyjne oraz technologie, takie jak np. internet oraz wirtualne systemy płatności, pozostające poza jakąkolwiek kontrolą instytucji

[353] J. Duży, *Zorganizowana przestępczość podatkowa w Polsce. Zwalczanie przestępczego nadużycia mechanizmów podatków VAT i akcyzowego*, Warszawa 2013.

[354] A. Damasiewicz, *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2010.

finansowych. Nowym zagrożeniem na styku realnych operacji finansowych i cyberprzestrzeni jest wykorzystywanie w procederze prania pieniędzy obrotu wirtualnymi walutami, np. bitcoins (BTC)[355].

8.5. Zarządzanie bezpieczeństwem instytucji finansowych

Wydaje się, że omówienie procesu zarządzania bezpieczeństwem instytucji finansowych należy rozpocząć od sformułowania definicji cechy bezpieczeństwa. Nie jest to zadanie łatwe, gdyż omawiane pojęcie można rozumieć na wiele sposobów, co znacząco utrudnia sformułowanie jednej, kompletnej definicji. Analiza pojęcia „bezpieczeństwa" w kontekście rynku finansowego pozwala wyróżnić cztery zasadnicze elementy związane z bezpieczeństwem rynków, czyli: bezpieczeństwo instytucji finansowych, bezpieczeństwo segmentów rynku finansowego, bezpieczeństwo transakcji oraz bezpieczeństwo klienta. Przez bezpieczeństwo instytucji finansowej należy rozumieć stan, w którym możliwe jest realizowanie jej zadań, a więc poprawne funkcjonowanie na rynku finansowym pomimo okresowych wahań koniunktury oraz różnego rodzaju szoków zewnętrznych. Omawiając zagadnienie bezpieczeństwa instytucji finansowej, należy wyróżnić jego aspekt wewnętrzny oraz zewnętrzny. W aspekcie zewnętrznym chodzi o stabilność systemu finansowego jako środowiska, w którym funkcjonują instytucje finansowe. Na bezpieczeństwo w aspekcie zewnętrznym składają się zatem regulacje nadzorcze oraz instytucje chroniące system finansowy przed destabilizacją. Mowa tu o takich konstrukcjach jak sieć bezpieczeństwa finansowego tworzona przez rządy, banki centralne, instytucje antyupadłościowe i instytucje nadzorcze. Bezpieczeństwo w aspekcie wewnętrznym można zdefiniować jako stabilność finansową, ekonomiczną i majątkową, umożliwiającą efektywne zarządzanie ryzykiem. Należy zauważyć, że instytucje finansowe zmuszone są zarządzać różnymi rodzajami ryzyka, takimi jak ryzyko operacyjne, ryzyko płynności, ryzyko kredytowe, ryzyko kapitałowe, ryzyko rynkowe, ryzyko ubezpieczenia. Wszystkie wskazane rodzaje ryzyka mają wpływ na bezpieczeństwo

[355] Z uwagi na charakter wykorzystywanej technologii szyfrującej oraz metod dokonywania transakcji system bitcoin zapewnia dużą anonimowość użytkowników.

instytucji finansowych, w szczególności na ich bezpieczeństwo finansowe, bezpieczeństwo bankowości elektronicznej, bezpieczeństwo środków pieniężnych, bezpieczeństwo systemów informatycznych, bezpieczeństwo informacji. Nie będzie przesadą stwierdzenie, że zarządzanie instytucjami finansowymi sprowadza się do zarządzania poszczególnymi rodzajami ryzyka w celu uniknięcia negatywnych skutków ich wystąpienia. Efektywne zarządzanie ryzykiem zapewnia w efekcie bezpieczeństwo instytucji finansowej. Bezpieczeństwo instytucji finansowych jest więc głównym uwarunkowaniem ich działalności, celem działalności, a także kryterium oceny ich funkcjonowania.

Przez zarządzanie ryzykiem bezpieczeństwa należy rozumieć przygotowywanie i wdrażanie przez instytucje finansowe odpowiednich procedur mających ograniczać zakłócenia funkcjonowania instytucji lub straty finansowe wynikłe z niezdolności do pełnej ochrony jej zasobów i informacji[356]. Przez niedostateczną ochronę zasobów należy rozumieć ochronę zasobów ludzkich, rzeczowych, kapitałowych, przez te ostatnie należy rozumieć środki pieniężne, co do których występuje ryzyko prania brudnych pieniędzy.

Instytucje finansowe obłożone są ustawowym obowiązkiem zarządzania ryzykiem bezpieczeństwa. Wśród środków bezpieczeństwa – bezwzględnego minimum, które instytucja finansowa powinna zastosować, wyróżnić należy[357]:

- identyfikację klienta i weryfikację jego tożsamości na podstawie dokumentów lub informacji publicznie dostępnych. W praktyce sprowadza się to do ustalenia i zapisania cech dokumentu stwierdzającego tożsamość osoby (dla osób fizycznych) lub zapisania aktualnych danych z wyciągu z rejestru sądowego (gdy mowa o osobach prawnych);
- zachowanie należytej staranności przy identyfikacji rzeczywistego beneficjenta i dostosowanie środków weryfikacji jego tożsamości do poziomu ryzyka. Identyfikacja powinna obejmować ustalenie struktury własności i zależności klienta;
- identyfikację celu klienta oraz charakteru stosunków gospodarczych, w których zamierza on pozostawać;

[356] K. Jajuga, *op. cit.*

[357] P. Kokot-Stępień, *Identyfikacja ryzyka jako kluczowy element zarządzania ryzykiem w przedsiębiorstwie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2015, nr 74, t. 1.

- kontrolę stosunków gospodarczych z klientem. Przez kontrolę należy tu rozumieć analizę zgodności transakcji przeprowadzanych przez klienta z profilem i ryzykiem jego działalności, badanie źródeł pochodzenia składników majątkowych oraz bieżącą aktualizację posiadanych informacji oraz dokumentów.

Należy podkreślić, że podczas identyfikacji konieczne jest zwracanie uwagi nie tylko na klientów instytucji finansowej, ale także na strony transakcji niebędące klientami instytucji. Uzyskane informacje dotyczące klienta i oraz pozostałych podmiotów będących stronami przeprowadzanych przez niego transakcji powinny być weryfikowane jeszcze przed zawarciem umowy z klientem lub przed przeprowadzeniem transakcji. Wymienione środki bezpieczeństwa finansowego winny być stosowane w poniższych przypadkach:

- przy zawieraniu umowy z klientem,
- przy przeprowadzaniu transakcji o wartości powyżej 15 000 euro, niezależnie od tego, czy mamy do czynienia z pojedynczą operacją czy szeregiem powiązanych operacji o mniejszej wartości indywidualnej,
- gdy istnieje uzasadnione podejrzenie, że dokonywana operacja służy w rzeczywistości praniu brudnych pieniędzy lub finansowania;
- gdy powzięte zostaną uzasadnione wątpliwości co do rzeczywistej tożsamości klienta[358].

Racjonalność w zarządzaniu bezpieczeństwem instytucji finansowej powinna się przejawiać w podzieleniu klientów instytucji finansowej na trzy grupy:

- klientów, w stosunku których należy stosować wszystkie wymienione środki bezpieczeństwa (zasada należytej staranności wobec klienta);
- klientów, wobec których instytucje finansowe mogą odstąpić od stosowania wszystkich środków bezpieczeństwa. To np. klienci będący podmiotami świadczącymi usługi finansowe, których siedziba znajduje się na terytorium Unii Europejskiej, a także klienci będący spółką notowaną na giełdzie;

[358] Dyrektywa 2005/60/WE Parlamentu Europejskiego i Rady z dnia 26 października 2005 r. w sprawie przeciwdziałania korzystaniu z systemu finansowego w celu prania pieniędzy oraz finansowania terroryzmu, Dz.Urz. UE, L 309/15, art. 7.

- klientów, wobec których uzasadnione jest zastosowanie wzmożonych środków bezpieczeństwa. Dla przykładu należy wskazać klientów nieobecnych (chodzi tu o obecność fizyczną instytucje mające swą siedzibę w innych krajach niż państwa członkowskie UE lub państwa, traktowane na mocy odrębnych umów jak państwa członkowskie oraz klientów zajmujących ważne polityczne stanowiska.

Przy dokonywaniu oceny ryzyka finansowania terroryzmu oraz prania brudnych pieniędzy należy uwzględnić cztery ustawowe kryteria:

- kryterium ekonomiczne, które można sprowadzić do oceny zgodności transakcji klienta z prowadzoną przez niego działalnością gospodarczą i jego aktywnością na rynku finansowym;
- kryterium geograficzne, polegające na zachowaniu ostrożności podczas dokonywania transakcji z klientami z państw strefy ryzyka, czyli państw, w których istnieje znaczne zagrożenie praniem brudnych pieniędzy i wspieraniem terroryzmu;
- kryterium przedmiotowe, polegające na ocenie działalności klienta pod kątem ryzyka prania pieniędzy i finansowania terroryzmu;
- kryterium behawioralne, sprowadzające się do oceny zachowania klienta pod względem jego nietypowości[359].

Niezwykle istotne z punktu widzenia zarządzania bezpieczeństwem w instytucji finansowej jest zapewnienie pracownikom udziału w szkoleniach specjalistycznych dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

8.6. Przeciwdziałanie przestępczości

Z uwagi na skomplikowanie zjawiska, jakim jest przestępczość gospodarcza, a także przyjęty w Polsce model rozproszonej ochrony i zapobiegania przestępczości konieczne było wytworzenie wielu aktów prawnych regulujących omawiane zagadnienie. Kluczowe znaczenie z punktu widzenia poszczególnych rynków mają przepisy regulujące zasady funkcjonowania

[359] Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2010 Nr 46, poz. 276 z późn. zm., art. 10a.

występujących podmiotów oraz kształtujące mechanizmy oraz procedury zapewniające bezpieczeństwo obrotu. W niektórych przypadkach regulacje te zawierają również przepisy karne (np. ustawa z dnia 19 sierpnia 1997 r. – Prawo bankowe[360]).

Zadania poszczególnych służb, organów i instytucji realizowane w zakresie przeciwdziałania i zwalczania przestępczości, w tym również tej o charakterze gospodarczym, zostały zawarte w ustawach kompetencyjnych (np. ustawie z dnia 6 kwietnia 1990 r. o Policji[361]).

Szczególną rolę w systemie przeciwdziałania i zwalczania przestępczości gospodarczej pełnią także przepisy odnoszące się do wymiany informacji pomiędzy poszczególnymi podmiotami ww. systemu (np. ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych[362]).

Niezwykle ważne z uwagi na przejrzystość oraz bezpieczeństwo obrotu są również regulacje określające obowiązki informacyjne podmiotów uczestniczących w obrocie finansowym (np. ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[363]).

Przepisy penalizujące poszczególne typy czynów zabronionych odnaleźć można w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny[364] oraz w ustawie z dnia 10 września 1999 r. – Kodeks karny skarbowy[365].

Do prowadzenia postępowań w sprawach z zakresu przestępczości gospodarczej zastosowanie znajdą natomiast przepisy ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy[366] oraz ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[367].

---

360 Dz.U. z 2012 r., poz. 1376 z późn. zm.
361 Dz.U. z 2011 r. Nr 287, poz. 1687 z późn. zm.
362 Dz.U. z 2006 r. Nr 216 z późn. zm.
363 Dz.U. z 2014 r., poz. 455.
364 Dz.U. z 1997 r. Nr 88, poz. 553 z późn. zm.
365 Dz.U. 1999 Nr 83, poz. 930 z późn. zm.
366 Dz.U. 1997 Nr 90, poz. 557 z późn. zm.
367 Dz.U. 1997 Nr 89, poz. 555 z późn. zm.

8.7. Podmioty przeciwdziałające przestępczości gospodarczej

Za podmiot, którego celem jest zapobieganie przestępczości w sferze gospodarki, uznać należy w szczególności[368]:

- **Ministra Finansów** – odgrywa kluczową rolę w zakresie przeciwdziałania i zwalczania przestępczości gospodarczej, zarówno z perspektywy procesu tworzenia i stosowania prawa (znaczna część regulacji istotnych w niniejszym zakresie pozostaje we właściwości tego organu), jak i w kontekście uprawnień posiadanych przez podległe mu struktury (od uprawnień o charakterze kontrolnym po czynności operacyjno-rozpoznawcze). Należy także zaznaczyć, ich prowadzona przez Ministra Finansów polityka fiskalna znajduje bezpośrednie przełożenie na trendy występujące w przestępczości gospodarczej;
- **Generalnego Inspektora Informacji Finansowej** – działa w zakresie przeciwdziałania praniu pieniędzy, badania przebiegu podejrzanych transakcji, wstrzymywania transakcji lub dokonywania blokady rachunków;
- **Generalnego Inspektora Kontroli Skarbowej** – sprawuje nadzór nad działalnością dyrektorów urzędów kontroli skarbowej, pracowników wywiadu skarbowego i komórek realizacyjnych;
- **Izby i urzędy skarbowe**;
- **Służbę Celną** – pełni istotną rolę przy zwalczaniu przestępstw związanych z wyłudzeniami VAT oraz nieuiszczaniem lub zaniżaniem należności publicznoprawnych;
- **Pełnomocnika Rządu do Spraw Zwalczania Nieprawidłowości Finansowych na Szkodę Rzeczypospolitej Polskiej lub Unii Europejskiej** – do jego zadań należy m.in. koordynowanie działań podejmowanych przez właściwe organy, mających na celu zabezpieczenie interesów finansowych RP lub UE;
- **Ministra Spraw Wewnętrznych** – odpowiedzialny za ochronę bezpieczeństwa i porządku publicznego. Prowadzi działania w odniesieniu do przestępczości gospodarczej zarówno bezpośrednio, m.in. poprzez przygotowywanie propozycji zmian systemowych o charakterze

[368] *Program przeciwdziałania i zwalczania przestępczości…*

prawnym i organizacyjnym pozwalających na podnoszenie skuteczności przeciwdziałania i zwalczania tej formy przestępczości, jak również pośrednio, poprzez realizowanie działań nadzorczych w odniesieniu do Policji i Straży Granicznej;

- **Policję** – prowadzi działania we wszystkich obszarach występowania przestępczości gospodarczej, wykorzystując w tym celu m.in. ofensywne metody pracy operacyjnej;
- **Straż Graniczną** – posiada w zakresie swojej właściwości uprawnienia do rozpoznawania, zapobiegania i wykrywania przestępstw i wykroczeń oraz ścigania ich sprawców. Straż Graniczna realizuje zadania zwalczania transgranicznej przestępczości gospodarczej, w zakresie swojej właściwości, wykorzystując w tym celu m.in. ofensywne metody pracy operacyjnej;
- **Agencję Bezpieczeństwa Wewnętrznego** – odpowiedzialna za rozpoznawanie, zapobieganie i wykrywanie najpoważniejszych przestępstw godzących w podstawy ekonomiczne państwa i jego bezpieczeństwo oraz ściganie ich sprawców;
- **Centralne Biuro Antykorupcyjne** – podejmuje działania zmierzające do przeciwdziałania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, podejmuje również działania w zakresie zwalczania działalności godzącej w interesy ekonomiczne państwa;
- **Prokuraturę** – prowadzi oraz nadzoruje postępowania przygotowawcze w sprawach karnych. W postępowaniach przed sądami prokuratorzy pełnią funkcję oskarżycieli publicznych;
- **Komisję Nadzoru Finansowego** – realizuje zadania w zakresie nadzoru nad rynkiem finansowym, w tym nad sektorem bankowym, rynkiem kapitałowym, ubezpieczeniowym, a także dotyczące nadzoru nad instytucjami płatniczymi i biurami usług płatniczych, instytucjami pieniądza elektronicznego oraz nad sektorem kas spółdzielczych;
- **Żandarmerię Wojskową** – do ścigania przestępstw gospodarczych popełnianych w Siłach Zbrojnych RP oraz w stosunku do żołnierzy, osób zatrudnionych w jednostkach wojskowych i osób przebywających na ich terenie, a także przedstawicieli sił zbrojnych państw obcych

i ich personelu cywilnego, jeśli umowy międzynarodowe nie stanowią inaczej, właściwa pozostaje Żandarmeria Wojskowa;
- **Służbę Kontrwywiadu Wojskowego** – realizuje zadania m.in. ochrony bezpieczeństwa produkcji i obrotu towarami, technologiami i usługami o przeznaczeniu wojskowym zamówionymi przez Sił Zbrojnych RP i inne jednostki organizacyjne Ministerstwa Obrony Narodowej.

Wskazać należy również, że w związku z uczestnictwem w Unii Europejskiej Polska zobowiązana jest wykonywać unijną politykę w obszarze zwalczania przestępczości, również o charakterze ekonomicznym. Wszelkie podejmowane inicjatywy wprowadzane są w życie na podstawie odpowiednich strategii i polityk UE. Ważna w tym zakresie pozostaje działalność podmiotów unijnych, w tym w szczególności Europejskiego Urzędu Policji – Europolu, do którego zadań należy pomoc organom ścigania krajów członkowskich w zwalczaniu przestępczości o charakterze transgranicznym. Europol umożliwia współpracę w zakresie wymiany informacji, zajmuje się także sporządzaniem analiz kryminalnych wspierających działania organów ścigania państw członkowskich, przygotowywaniem raportów strategicznych, wsparciem technicznym prowadzonych śledztw i dochodzeń prowadzonych na terenie UE pod nadzorem państw członkowskich. Europol działa również na rzecz implementacji Operacyjnych Planów Działań (OAPs) realizowanych przez projekty EMPACT (*European Multidisciplinary Platform Against Crime Threats*) w ramach Polityki Bezpieczeństwa UE. Polska jednostka Europolu ma siedzibę w Komendzie Głównej Policji. Z pomocy Europolu korzystają również inne służby.

Kolejnym podmiotem, ważnym w praktyce przeciwdziałania i zwalczania przestępczości ekonomicznej, jest OLAF – Europejskie Biuro ds. Zwalczania Nadużyć Finansowych, do którego celów należy chronienie interesów finansowych Unii w drodze zwalczania nadużyć finansowych, korupcji oraz wszelkich innych działań niezgodnych z prawem[369]. OLAF ma również za zadanie prowadzenie dochodzeń w sprawie uchybień ze strony ich członków instytucji unijnych, ich pracowników, które mogą prowadzić do postępowań administracyjnych lub karnych. OLAF zapewnia również wsparcie dla

[369] Prezentacja OLAF-u, Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych, http://europa.eu/pol/index_pl.htm [dostęp: 15.05.2019].

Komisji Europejskiej w procesie formułowania i wdrażania procedur przeciwdziałających nadużyciom finansowym. Biuro to posiada uprawnienia do prowadzenia dochodzeń wewnętrznych, wśród organów UE, oraz zewnętrznych, krajowych, dotyczących środków budżetowych UE[370]. OLAF dysponuje również siecią informacyjną, będącą skutecznym narzędziem wymiany informacji o podmiotach prowadzących działalność gospodarczą na terenie Unii. Z kolei organizacją dedykowaną współpracy Państw Członkowskich UE w zakresie prowadzenia postępowań przygotowawczych w sprawach karnych jest Europejska Jednostka Współpracy Sądowej (Eurojust). Do zadań Eurojustu należy zwiększenie skuteczności krajowych organów śledczych i dochodzeniowych w sprawach dotyczących przestępczości poważnej i zorganizowanej o charakterze transgranicznym, wspieranie pomocy prawnej na etapie postępowania sądowego, rozstrzyganie konfliktów w zakresie jurysdykcji w toku postępowań, w których więcej niż jeden krajowy organ wymiaru sprawiedliwości ma możliwość prowadzenia działań dochodzeniowych lub śledczych w danej sprawie. W kontekście zwalczania transgranicznej przestępczości gospodarczej ograniczoną rolę odgrywa również współpraca Straży Granicznej z Frontex – Europejską Agencją Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych Państw Członkowskich Unii Europejskiej, do której zadań należy m.in. pomoc w szkoleniu służb granicznych.

Poza uczestniczeniem w strukturach UE polska administracja wykorzystuje także możliwości współpracy międzynarodowej w zakresie zwalczania przestępczości gospodarczej[371]. Duże znaczenie posiada w tym kontekście Międzynarodowa Organizacja Policji Kryminalnej – Interpol. Jest to instytucja powołana w zamiarze zapewnienia współpracy międzynarodowej w zwalczaniu przestępczości. Skupia ok. 190 krajów członkowskich. Do priorytetów Interpolu należy m.in. zwalczanie przestępczości zorganizowanej i ekonomicznej. Do zadań Organizacji zalicza się identyfikację trendów, szlaków przemytniczych i zorganizowanych grup przestępczych, gromadzenie

[370] K. Dziadek, *Kontrola jako narzędzie wykrywania nieprawidłowości w wykorzystaniu funduszy unijnych,* „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2011, nr 669.

[371] M. Smolak, *Formy zwalczania procederu prania brudnych pieniędzy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9; B. Jagodziński, *Rola wywiadu finansowego w przeciwdziałaniu procederowi prania pieniędzy i w jego zwalczaniu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7.

i analizę danych otrzymanych z krajów członkowskich oraz przygotowywanie raportów czy pomoc członkom w prowadzeniu międzynarodowych śledztw oraz opracowywanie i publikowanie listów gończych. Interpol dysponuje infrastrukturą komunikacyjną łączącą Sekretariat Generalny z Krajowymi Biurami Interpolu w krajach członkowskich, a także posiada dostęp do różnych baz danych. Na uwagę zasługuje również działalność Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (FATF), będącej międzyrządowym ciałem powołanym do życia w 1989 r. podczas szczytu G7, którego zadaniem jest przygotowywanie i wspieranie działań służących zwalczaniu procederu prania pieniędzy i finansowania terroryzmu, a także ustalanie i badanie standardów legislacyjnych i organizacyjnych[372]. Standardy FATF są powszechnie respektowane na arenie międzynarodowej oraz propagowane i weryfikowane przez powołane do tego instytucje. Polska, mimo że nie jest członkiem FATF – jest konfrontowana z zaleceniami i bierze udział w ich tworzeniu i weryfikacji na forum Unii Europejskiej i Komitetu Specjalnego Ekspertów Rady Europy ds. Oceny Środków Przeciwdziałania Praniu Pieniędzy w Krajach Europy Środkowej i Wschodniej (MONEYVAL). W 2010 roku kraje UE utworzyły sieć Eurofisc, której celem jest wymiana danych między państwami członkowskimi umożliwiających współpracę w zakresie zwalczania oszustw w dziedzinie VAT. Zgodnie z ideą Eurofisc badaniem obejmowani są przede wszystkim podatnicy, sklasyfikowani jako podmioty wysokiego ryzyka dokonujący transakcji wewnątrzwspólnotowych w zakresie dostaw bądź świadczenia usług, których odbiorcą są, z wysokim prawdopodobieństwem, podatnicy uczestniczący w oszustwie „karuzelowym" lub oszustwie typu „znikający podatnik" w innych państwach członkowskich UE.

8.8. Sposoby przeciwdziałania przestępczości

Analizy groźnego zjawiska, jakim bez wątpienia jest przestępczość gospodarcza, muszą prowadzić do wypracowywania skutecznych mechanizmów jej przeciwdziałania. Wymaga to opracowania odpowiedniej strategii

[372] *Financial Action Task Force – Groupe d'action financiere, Trade Based Money Laundering*, Paryż 2006.

ustawodawczej oraz użycia odpowiednich instrumentów prawnych (np. kontroli czy rejestrów), jak też rozpoznawania i eliminowania czynników sprzyjających występowaniu przestępczości. Realizacja tak sformułowanego celu wymaga ścisłej współpracy organów ścigania, organizacji reprezentujących podmioty szczególnie narażone na ryzyko przestępczości oraz administracji publicznej[373]. Współpraca wymienionych trzech kategorii podmiotów winna się przejawiać w szczególności w opracowywaniu efektywnych rozwiązań prawnych służących identyfikacji zagrożeń oraz wymianie informacji i doświadczeń.

Jako jedną z możliwych do przyjęcia strategii przeciwdziałania przestępczości należy wskazać tzw. metodę administracyjną. Przyjęcie wspomnianej metody przejawia się w wykorzystywaniu instrumentów prawno-administracyjnych celem ograniczania swobody działalności przestępczej poprzez np. wprowadzenie stosownych wymogów dotyczących ewidencjonowania operacji, a także przekazanie odpowiednich środków sprawowania kontroli w ręce uprawnionych organów administracji. Fundamentalne znaczenie ma również wypracowanie skutecznych rozwiązań prawnych, zapobiegających powstawaniu okazji wykorzystywanych następnie przez przestępców. Dobrym przykładem takich zmian w prawie może być np. stworzenie katalogu towarów szczególnie narażonych na wykorzystywanie w procederze wyłudzania podatków oraz skrócenie okresu rozliczenia podatku VAT w stosunku do obrotu tymi towarami, a także stosowanie mechanizmu odwrotnego obciążenia (*reverse charge mechanism*). Równie istotna wydaje się potrzeba zmiany sposobu naliczania i odliczania podatku VAT obciążająca obowiązkiem jego odprowadzania tego, kto ostatecznie nabył dany towar – takie rozwiązanie znacząco ograniczyłoby możliwość występowania przez sprzedawców do urzędów skarbowych o zwrot podatków[374]. Należy również podkreślić konieczność zachowania proporcjonalności przy obciążaniu legalnie działających podmiotów obowiązkami informacyjnymi i kontrolnymi tak, aby umożliwić im efektywne ekonomicznie wykonywanie działalności. Działania podmiotów prowadzących swą działalność legalnie charakteryzują się, z samej

[373] F. Schneider, K. Raczkowski, *Sfera nieoficjalna w gospodarce*, „Infos" 2013, nr 158.

[374] E. Małecka-Ziembińska, *Luka w podatku od towarów i usług oraz sposoby jej ograniczania*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace / Szkoła Główna Handlowa" 2017, nr 1.

natury sformułowanych przez te podmioty celów i środków ich osiągnięcia, wolą czynienia zadość obowiązkom administracyjnym. Nie wymaga natomiast szczególnej przenikliwości konstatacja, że podmioty prowadzące działalność przestępczą nie mają woli wypełniania wspomnianych obowiązków w ogóle. W związku z powyższymi rozważaniami należy podkreślić, że przepisy administracyjne mają fundamentalne znaczenie dla zwalczania przestępczości ekonomicznej. To właśnie przepisy administracyjne stanowią podstawę prowadzenia przez organy podatkowe lub kontroli skarbowej działań dążących do stwierdzenia wystąpienia nieprawidłowości, szczególnie zaś związanej z wyłudzeniami VAT oraz niewywiązywaniem się z obowiązku opłacania należności publicznoprawnych. Metoda administracyjna sprowadza się zatem do samodzielnych działań organów administracyjnych oraz do ich bezpośredniej współpracy z organami ścigania. Na mocy przepisów administracyjnych można również zobowiązać wszystkie instytucje działające w ramach administracji do aktywnego wspierania realizacji funkcji kontrolnej przez organy upoważnione. Jako przykład właściwej realizacji postulatu wspierania działalności tych organów należy wskazać uprawnienie organów ścigania do korzystania w swej działalności z instrumentów administracyjnych, np. uzyskiwania dostępu do informacji będących w posiadaniu różnych organów administracji publicznej, użytecznych z perspektywy ścigania sprawców przestępstw.

Należy zauważyć, że przestępczość ekonomiczna oddziałuje negatywnie nie tylko na budżet państwa, ale również na budżety prywatne. Skutkami tego rodzaju przestępczości są m.in. straty finansowe przedsiębiorstw. Przestępstwa te mogą mieć zarówno charakter pośredni, jak i bezpośredni. Przestępstwa o charakterze pośrednim to np. nielegalne wprowadzanie do obrotu towarów chronionych prawem autorskim lub patentowym, a także tańszych odpowiedników oryginalnych produktów kosztem zaniżania należności publicznoprawnych, co ma efekt w postaci spadku popytu na towary wytwarzane i sprzedawane zgodnie z prawem. Przestępstwa o charakterze bezpośrednim to natomiast czyny takie jak wyłudzenia ubezpieczeń lub kredytów. W działania przestępców nierzadko zostają wplątane również legalnie prosperujące przedsiębiorstwa. Przestępcy mogą dokonywać przestępstw wprost na szkodę tych przedsiębiorstw lub też mogą korzystać z nich jako narzędzi służących prowadzeniu działalności sprzecznej z prawem. Zdarza się, że legalnie działające

podmioty gospodarcze są wykorzystywane np. do prania brudnych pieniędzy albo przewozu nielegalnych towarów. Wydaje się jednak zasadne, aby na potrzeby niniejszego omówienia rozróżnić sytuacje, w których podmiot jest tworzony lub przejmowana jest nad nim kontrola w celu prowadzenia za jego pośrednictwem działalności sprzecznej z prawem, od podmiotów gospodarczych wykorzystywanych do działalności przestępczej bez wiedzy i woli ich właścicieli (co ma często miejsce przy wyłudzaniu podatku VAT)[375]. Należy podkreślić, że sektor prywatny może i powinien współpracować z organami ścigania nie tylko w celu obniżenia częstotliwości występowania sytuacji sprzyjających popełnianiu przestępstw ekonomicznych, ale również w ściganiu i zwalczaniu przestępstw już popełnionych. Dobrym przykładem takiej współpracy jest możliwość pozyskiwania przez organy ścigania informacji pozostających w posiadaniu lub możliwych do uzyskania organizacji reprezentujących interesy przedsiębiorców. Współdziałanie sektora publicznego i prywatnego może się przejawiać również w tworzeniu baz danych i rejestrów zawierających informacje posiadane przed podmioty prywatne oraz umożliwianiu organom ścigania dostępu do tych informacji, przy pełnym wszakże poszanowaniu ochrony danych osobowych i innych obowiązujących w tym zakresie regulacji. Wielką wartością podmiotów prywatnych, jaką mają do zaoferowania organom ścigania, jest również dostęp do specjalistycznej wiedzy. Pomoc tych podmiotów, przejawiająca się w prowadzeniu wspólnych programów szkoleniowych, określaniu metod działania sprawców przestępstw ekonomicznych, wypracowywaniu skutecznych instrumentów przeciwdziałania nieprawidłowościom czy wreszcie monitorowaniu trendów przestępczości, jest trudna do przecenienia. Umożliwienie tego rodzaju współpracy wymaga jednak stworzenia różnego rodzaju platform komunikacji dla podmiotów sektora publicznego i prywatnego. Wytworzenie instytucji prawnych umożliwiających korzystanie z wiedzy ekspertów sektora prywatnego w procesie przeciwdziałania przestępczości ekonomicznej jawi się jako jedno z najważniejszych zadań stojących współcześnie przed ustawodawcą.

[375] T. Juja, *Wydajność fiskalna podatku od towarów i usług w latach 2001–2007*, [w:] *Współczesne finanse. Stan i perspektywy rozwoju finansów publicznych*, red. J. Głuchowski, Toruń 2008.

ROZDZIAŁ DZIEWIĄTY

Założenia projektowe oraz analiza *de lege lata* typów czynów zabronionych w obszarze finansowym w Polsce

9.1. Założenia projektowe

Przedstawione poniżej i zawierające się w tym podrozdziale rozważania dotyczą założeń projektowych pełnego przedmiotu prac podejmowanych w ramach projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" w kontekście rynku finansowego. W związku z tym celowe było zaprezentowanie całościowego przekroju płaszczyzny badawczej rynku finansowego i wytycznych dotyczących podejmowanych prac oraz zastosowanej metodologii. Natomiast zagadnienia merytoryczne zawarte w niniejszej monografii naukowej stanowią jeden z licznych, choć istotny, etapów podejmowanych zaawansowanych prac naukowych. Opracowanie prezentuje wybrane i najciekawsze rezultaty analiz Zespołu Implementacyjnego w kontekście korelacji prawa, gospodarki i technologii na rzecz zapobiegania przyczynom przestępczości w obszarze rynku finansowego.

9.1.1. Płaszczyzna badawcza

Analiza przyczyn powstawania sytuacji, w których dochodzi do przestępstw w obszarze rynku finansowego, stanowiła główny obszar badawczy oraz analityczny pryzmat dla projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości"[376] w obszarze rynku

[376] Oficjalna strona internetowa projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości": https://iws.gov.pl/projekt/ [dostęp: 15.05.2019].

finansowego. Natomiast opracowanie rozwiązań czy możliwość wykorzystania produktów oraz usług przybrały postać głównych ram badawczych.

W związku z powyższym w kontekście prac związanych z badaniem rynku finansowego dokonano podejścia analitycznego dotyczącego zarządzania instytucjami finansowymi z wykorzystaniem technologii utrudniających dokonywanie przestępstw w tym zakresie. Co istotne, podejmowane kompleksowe działania naukowe przyjęły pozycję u źródła problemu, a więc koncentrowały się na kwestii zarządzania instytucjami finansowymi oraz ocenie poziomu zaawansowania i zakresu wykorzystania technologii utrudniających dokonywanie przestępstw finansowych w tych podmiotach. Dodatkowo, w ramach prowadzonych badań została pozyskana, a także zaktualizowana wiedza na temat zagranicznych rozwiązań w dziedzinie finansów oraz zagrożeń dla podstawowych zasad polskiego porządku prawnego.

Analiza rynku finansowego została oparta na systemie czterech modułów tematycznych. Pierwszy z nich to Assessing Foundations[377], w ramach którego zajęto się kwestiami zarządzania strategicznego, zarządzania ludźmi w organizacji i podejmowania decyzji, zarządzania ryzykiem oraz analizy problemu przestępczości w sektorze finansowym. Drugi to Improving Performance[378], w ramach którego zajęto się kwestiami zarządzania operacjami w sektorze finansowym, kreatywności i innowacyjności w zarządzaniu, nowych technologii integrujących informacje w zarządzaniu, operacjami oraz dostępności na świecie rozwiązań problemów przestępczości w sektorze finansowym. Trzeci to Transforming People and Organizations[379], w ramach którego omówiono kwestie bezpieczeństwa cybernetycznego w bankowości, wdrażania strategii biznesowych, zarządzania zmianą oraz wdrożenia rozwiązań dla sektora finansowego w Polsce. Zaś czwarty to Heading Into the Future[380], w ramach którego rozważono kwestie budowania kultury organizacyjnej wspierającej postawy praworządności, tworzenia strategicznych scenariuszy na przyszłość,

[377] Moduł Assessing Foundations polegał na zidentyfikowaniu problemu przestępczości w Polsce w świetle wybranych sektorów polskiej gospodarki.

[378] Moduł Improving Performance polegał na znalezieniu rozwiązań zidentyfikowanych problemów.

[379] Moduł Transforming People & Organisations polegał na przybliżeniu, w jaki sposób te rozwiązania mogą zmieniać organizacje i ludzkie zachowania.

[380] Moduł Heading into the Future polegał na debatowaniu nad przyszłością i przyszłymi zmianami np. technologicznymi.

innowacyjnych strategii rozwoju gospodarczego oraz przygotowania na nowe rodzaje przestępstw w sektorze finansowym w przyszłości.

9.1.2. Wytyczne dotyczące podejmowanych prac

Tworzone rekomendacje, wytyczne oraz spodziewane wymierne rezultaty skoncentrowały się wokół siedmiu podstawowych segmentów analitycznych stanowiących cele subsydiarne części projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości" poświęconej rynkowi finansowemu. Pierwszy z nich to analiza rozwiązań organizacyjnych ułatwiających zachowanie kontroli instytucji finansowej nad operacjami realizowanymi przez jej pracowników. Drugi to analiza procesu podejmowania decyzji, trzeci – analiza zarządzania operacjami w instytucjach finansowych, czwarty – analiza zarządzania ryzykiem w instytucjach finansowych, piąty – analiza przygotowania obrony przed różnymi formami ataków na instytucje finansowe, szósty – działalność międzynarodowych grup przestępczych oraz metody zapobiegania im w instytucjach finansowych, a siódmy to przestępstwa finansowe dokonywane przez klientów instytucji finansowych oraz metody zapobiegania im. Projektowane rozwiązania cechują się wysokim stopniem innowacyjności, perspektywy zastosowania, kompatybilności oraz praktyczności. Reasumując, poprzez zbadanie celów subsydiarnych uwidoczniono główny cel niniejszej części projektu. Natomiast każde podejmowane działanie w ramach projektu oceniane było z punktu widzenia głównego celu oraz głównych ram badawczych, a sami badacze starali się je wypełnić i zmierzać do stworzenia rekomendacji czy wytycznych oraz osiągać wymierne rezultaty, które znajdą zastosowanie zarówno w teorii, jak i praktyce.

Układ zaproponowanych priorytetów projektu w zakresie analizy rynku finansowego w kontekście korelacji prawa, gospodarki i technologii na rzecz zapobiegania przyczynom przestępczości brał pod uwagę wychodzenie od niezbędnych badań podstawowych, poprzez badania aplikacyjne, dochodząc do prac rozwojowych (używana nomenklatura jest zgodna z ustawą z dnia

20 lipca 2018 r. – Prawo o szkolnictwie wyższym[381]). Cały porządek zaproponowanych prac zmierzał do analizy wpływu innowacji w obszarze rynku finansowego, która ma przybierać postać zastosowania nowoczesnych technologii do użytku praktycznego. Zauważono, że ciekawym rodzajem nowych technologii w sektorze finansowym jest szeroko rozumiane zastosowanie walut wirtualnych[382]. Niemniej jednak wpływ innowacji należy postrzegać przez pryzmat głównego celu niniejszej części projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości", którym to jest analiza przyczyn powstawania sytuacji, gdy dochodzi do przestępstw w obszarze rynku finansowego.

- Właściwe jest przypisanie szczególnej uwagi aspektom ochrony praw człowieka w kontekście badanej materii. Zasadniczym pytaniem, jakie się pojawia, jest dylemat, czy wymierne rezultaty oraz produkty innowacji są zgodne w swojej substancji z newralgicznymi prawami każdego człowieka. W związku z tym zakres przyszłych regulacji, które mogą zostać zaproponowane (w szczególności z uwagi na nakierunkowanie materii na zapobieganie przyczynom przestępczości), należy konfrontować z zakresem i wykładnią regulacji z zakresu konstytucyjnej ochrony praw i wolności (Konstytucja Rzeczypospolitej Polskiej[383]) oraz europejskiej ochrony praw człowieka (1. Unia Europejska – Karta

[381] Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2018 r., poz. 1668, 2024, 2245; z 2019 r., poz. 276).

[382] M. Brière, K. Oosterlinck, A. Szafarz, *Virtual Currency, Tangible Return. Portfolio Diversification with Bitcoin*, „Journal of Asset Management" 2015, no.16(6), s. 365–373; M. Kubát, *Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value*, „Procedia Economics and Finance" 2015, no. 30, s. 409–416; A. Dibrova, *Virtual Currency. New Step in Monetary Development*, „Procedia – Social and Behavioral Sciences" 2016, no. 229, s. 42–49; S. Brown, *Cryptocurrency and Criminality. The Bitcoin Opportunity*, „The Police Journal: Theory, Practice and Principles" 2016, no. 89(4), s. 327–339; Europejski Bank Centralny, *Virtual Currency Schemes*, Frankfurt nad Menem 2012; The Financial Action Task Force Report, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, Paryż 2014; European Banking Authority, *EBA Opinion on „virtual currencies"*, Londyn 2014.

[383] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483; z 2001 r. Nr 28, poz. 319; z 2006 r. Nr 200, poz. 1471; z 2009 r. Nr 114, poz. 946).

Praw Podstawowych Unii Europejskiej[384]; 2. Rada Europy – Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności[385]), w szczególności z Prawem do wolności i bezpieczeństwa osobistego, które znalazło swoje odwzorowanie w art. 41 KRP, art. 6 KPP UE (Prawo do wolności i bezpieczeństwa osobistego), w art. 5 EKPC (Prawo do wolności i bezpieczeństwa osobistego).

Art. 41 Konstytucji Rzeczypospolitej Polskiej	1. Każdemu zapewnia się nietykalność osobistą i wolność osobistą. Pozbawienie lub ograniczenie wolności może nastąpić tylko na zasadach i w trybie określonych w ustawie; 2. Każdy pozbawiony wolności nie na podstawie wyroku sądowego ma prawo odwołania się do sądu w celu niezwłocznego ustalenia legalności tego pozbawienia. O pozbawieniu wolności powiadamia się niezwłocznie rodzinę lub osobę wskazaną przez pozbawionego wolności; 3. Każdy zatrzymany powinien być niezwłocznie i w sposób zrozumiały dla niego poinformowany o przyczynach zatrzymania. Powinien on być w ciągu 48 godzin od chwili zatrzymania przekazany do dyspozycji sądu. Zatrzymanego należy zwolnić, jeżeli w ciągu 24 godzin od przekazania do dyspozycji sądu nie zostanie mu doręczone postanowienie sądu o tymczasowym aresztowaniu wraz z przedstawionymi zarzutami; 4. Każdy pozbawiony wolności powinien być traktowany w sposób humanitarny; 5. Każdy bezprawnie pozbawiony wolności ma prawo do odszkodowania.
Art. 6 Karty Praw Podstawowych Unii Europejskiej	Każdy ma prawo do wolności i bezpieczeństwa osobistego.
Art. 5 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	1. Każdy ma prawo do wolności i bezpieczeństwa osobistego. Nikt nie może być pozbawiony wolności, z wyjątkiem następujących przypadków i w trybie ustalonym przez prawo: a) zgodnie z prawem pozbawienia wolności w wyniku skazania przez właściwy sąd; b) zgodnego z prawem zatrzymania lub aresztowania w przypadku niepodporządkowania się wydanemu zgodnie z prawem orzeczeniu sądu lub w celu zapewnienia wykonania określonego w ustawie obowiązku; c) zgodnego z prawem zatrzymania lub aresztowania w celu postawienia przed właściwym organem, jeżeli istnieje uzasadnione podejrzenie popełnienia czynu zagrożonego karą lub jeśli jest to konieczne w celu zapobieżenia popełnienia takiego czynu lub uniemożliwienia ucieczki po jego dokonaniu; d) pozbawienia nieletniego wolności na podstawie zgodnego z prawem orzeczenia w celu ustanowienia nadzoru wychowawczego lub zgodnego z prawem pozbawienia nieletniego wolności w celu postawienia go przed właściwym organem; e) zgodnego z prawem pozbawienia wolności osoby w celu zapobieżenia szerzeniu przez nią choroby zakaźnej, osoby umysłowo chorej, alkoholika, narkomana lub włóczęgi; f) zgodnego z prawem zatrzymania lub aresztowania osoby w celu zapobieżenia jej nielegalnemu wkroczeniu na terytorium państwa lub osoby, przeciwko której toczy się postępowanie o wydalenie lub ekstradycję.

[384] Karta Praw Podstawowych Unii Europejskiej (Dziennik Urzędowy Unii Europejskiej C 326, 26.10.2012, s. 391–407).

[385] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności (Dz.U. 1993 Nr 61, poz. 284).

	2. Każdy, kto został zatrzymany, powinien zostać niezwłocznie i w zrozumiałym dla niego języku poinformowany o przyczynach zatrzymania i o stawianych mu zarzutach. 3. Każdy zatrzymany lub aresztowany zgodnie z postanowieniami ust. 1 lit. c) niniejszego artykułu powinien zostać niezwłocznie postawiony przed sędzią lub innym urzędnikiem uprawnionym przez ustawę do wykonywania władzy sądowej i ma prawo być sądzony w rozsądnym terminie albo zwolniony na czas postępowania. Zwolnienie może zostać uzależnione od udzielenia gwarancji zapewniających stawienie się na rozprawę. 4. Każdy, kto został pozbawiony wolności przez zatrzymanie lub aresztowanie, ma prawo odwołania się do sądu w celu ustalenia bezzwłocznie przez sąd legalności pozbawienia wolności i zarządzenia zwolnienia, jeżeli pozbawienie wolności jest niezgodne z prawem. 5. Każdy, kto został pokrzywdzony przez niezgodne z treścią tego artykułu zatrzymanie lub aresztowanie, ma prawo do odszkodowania.

- Prawem do rzetelnego procesu sądowego, które znalazło swoje odwzorowanie w art. 45 KRP, art. 42 KRP, art. 47 (Prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu) i 48 (Domniemanie niewinności i prawo do obrony) KPP UE oraz art. 6 (Prawo do rzetelnego procesu sądowego) EKPC.

Art. 45 Konstytucji Rzeczypospolitej Polskiej	1. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki przez właściwy, niezależny, bezstronny i niezawisły sąd. 2. Wyłączenie jawności rozprawy może nastąpić ze względu na moralność, bezpieczeństwo państwa i porządek publiczny oraz ze względu na ochronę życia prywatnego stron lub inny ważny interes prywatny. Wyrok ogłaszany jest publicznie.
Art. 42 Konstytucji Rzeczypospolitej Polskiej	1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu.
Art. 47 Karty Praw Podstawowych Unii Europejskiej	Każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w niniejszym artykule. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony uprzednio na mocy ustawy. Każdy ma możliwość uzyskania porady prawnej, skorzystania z pomocy obrońcy i przedstawiciela. Pomoc prawna jest udzielana osobom, które nie posiadają wystarczających środków, w zakresie w jakim jest ona konieczna dla zapewnienia skutecznego dostępu do wymiaru sprawiedliwości.
Art. 48 Karty Praw Podstawowych Unii Europejskiej	1. Każdego oskarżonego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona zgodnie z prawem. 2. Każdemu oskarżonemu gwarantuje się poszanowanie prawa do obrony.

Art. 6 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	1. Każdy ma prawo do sprawiedliwego i publicznego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony ustawą przy rozstrzyganiu o jego prawach i obowiązkach o charakterze cywilnym albo o zasadności każdego oskarżenia w wytoczonej przeciwko niemu sprawie karnej. Postępowanie przed sądem jest jawne, jednak prasa i publiczność mogą być wyłączone z całości lub części rozprawy sądowej ze względów obyczajowych, z uwagi na porządek publiczny lub bezpieczeństwo państwowe w społeczeństwie demokratycznym, gdy wymaga tego dobro małoletnich lub gdy służy to ochronie życia prywatnego stron albo też w okolicznościach szczególnych, w granicach uznanych przez sąd za bezwzględnie konieczne, kiedy jawność mogłaby przynieść szkodę interesom wymiaru sprawiedliwości. 2. Każdego oskarżonego o popełnienie czynu zagrożonego karą uważa się za niewinnego do czasu udowodnienia mu winy zgodnie z ustawą. 3. Każdy oskarżony o popełnienie czynu zagrożonego karą ma co najmniej prawo do: a) niezwłocznego otrzymania szczegółowej informacji w języku dla niego zrozumiałym o istocie i przyczynie skierowanego przeciwko niemu oskarżeniu; b) posiadania odpowiedniego czasu i możliwości do przygotowania obrony; c) bronienia się osobiście lub przez ustanowionego przez siebie obrońcę, a jeśli nie ma wystarczających środków na pokrycie kosztów obrony, do bezpłatnego korzystania z pomocy obrońcy wyznaczonego z urzędu, gdy wymaga tego dobro wymiaru sprawiedliwości; d) przesłuchania lub spowodowania przesłuchania świadków oskarżenia oraz żądania obecności i przesłuchania świadków obrony na takich samych warunkach jak świadków oskarżenia; e) korzystania z bezpłatnej pomocy tłumacza, jeżeli nie rozumie lub nie mówi językiem używanym w sądzie.

- Prawem do podstawy prawnej karania, które znalazło swoje odwzorowanie w art. 41 KRP, art. 49 KPP UE (Zasady legalności oraz proporcjonalności kar do czynów zabronionych pod groźbą kary) oraz art. 7 EKPC (Zakaz karania bez podstawy prawnej).

Art. 42 Konstytucji Rzeczypospolitej Polskiej	1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu.
Art. 49 Karty Praw Podstawowych Unii Europejskiej	1. Nikt nie może zostać skazany za popełnienie czynu polegającego na działaniu lub zaniechaniu, który według prawa krajowego lub prawa międzynarodowego nie stanowił czynu zabronionego pod groźbą kary w czasie jego popełnienia. Nie wymierza się również kary surowszej od tej, którą można było wymierzyć w czasie, gdy czyn zabroniony pod groźbą kary został popełniony. Jeśli ustawa, która weszła w życie po popełnieniu czynu zabronionego pod groźbą kary, przewiduje karę łagodniejszą, ta właśnie kara ma zastosowanie. 2. Niniejszy artykuł nie stanowi przeszkody w sądzeniu i karaniu osoby za działanie lub zaniechanie, które w czasie, gdy miało miejsce, stanowiło czyn zabroniony pod groźbą kary, zgodnie z ogólnymi zasadami uznanymi przez wspólnotę narodów. 3. Kary nie mogą być nieproporcjonalnie surowe w stosunku do czynu zabronionego pod groźbą kary.

Art. 7 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	1. Nikt nie może być uznany za winnego popełnienia czynu polegającego na działaniu lub zaniechaniu działania, który według prawa wewnętrznego lub międzynarodowego nie stanowił czynu zagrożonego karą w czasie jego popełnienia. Nie będzie również wymierzona kara surowsza od tej, którą można było wymierzyć w czasie, gdy czyn zagrożony karą został popełniony. 2. Niniejszy artykuł nie stanowi przeszkody w sądzeniu i karaniu osoby winnej działania lub zaniechania, które w czasie popełnienia stanowiły czyn zagrożony karą według ogólnych zasad uznanych przez narody cywilizowane.

- Prawem do poszanowania życia prywatnego i rodzinnego, które znalazło swoje odwzorowanie w art. 47 KRP art. 7 KPP UE (Poszanowanie życia prywatnego i rodzinnego) oraz art. 8 EKPC (Prawo do poszanowania życia prywatnego i rodzinnego).

Art. 47 Konstytucji Rzeczypospolitej Polskiej	Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.
Art. 7 Karty Praw Podstawowych Unii Europejskiej	Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się.
Art. 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. 2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób.

- Prawem do ochrony danych osobowych, które znalazło swoje odwzorowanie w art. 8 KPP UE (Ochrona danych osobowych) oraz pośrednio w art. 51 KRP.

Art. 51 Konstytucji Rzeczypospolitej Polskiej	1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.
Art. 8 Karty Praw Podstawowych Unii Europejskiej	1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą. 2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. 3. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

- Prawem do wolności opinii i informacji, które znalazło swoje odwzorowanie w art. 54 KRP, art. 11 KPP UE (Wolność wypowiedzi i informacji) oraz w art. 10 EKPC (Wolność wyrażania opinii).

Art. 54 Konstytucji Rzeczypospolitej Polskiej	1. Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. 2. Cenzura prewencyjna środków społecznego przekazu oraz koncesjonowanie prasy są zakazane. Ustawa może wprowadzić obowiązek uprzedniego uzyskania koncesji na prowadzenie stacji radiowej lub telewizyjnej.
Art. 11 Karty Praw Podstawowych Unii Europejskiej	1. Każdy ma prawo do wolności wypowiedzi. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. 2. Szanuje się wolność i pluralizm mediów.
Art. 10 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	1. Każdy ma prawo do wolności wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Niniejszy przepis nie wyklucza prawa Państw do poddania procedurze zezwoleń przedsiębiorstw radiowych, telewizyjnych lub kinematograficznych. 2. Korzystanie z tych wolności pociągających za sobą obowiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej.

- Prawem do wolności zgromadzeń i stowarzyszania się, które znalazło swoje odwzorowanie w art. 57 KRP, art. 58 KRP, art. 59 KRP, art. 12 KPP UE (Wolność zgromadzania się i stowarzyszania się) oraz w art. 11 EKPC (Wolność zgromadzeń i stowarzyszania się).

Art. 57 Konstytucji Rzeczypospolitej Polskiej	Każdemu zapewnia się wolność organizowania pokojowych zgromadzeń i uczestniczenia w nich. Ograniczenie tej wolności może określać ustawa.
Art. 58 Konstytucji Rzeczypospolitej Polskiej	1. Każdemu zapewnia się wolność zrzeszania się. 2. Zakazane są zrzeszenia, których cel lub działalność są sprzeczne z Konstytucją lub ustawą. O odmowie rejestracji lub zakazie działania takiego zrzeszenia orzeka sąd. 3. Ustawa określa rodzaje zrzeszeń podlegających sądowej rejestracji, tryb tej rejestracji oraz formy nadzoru nad tymi zrzeszeniami.

Art. 59 Konstytucji Rzeczypospolitej Polskiej	1. Zapewnia się wolność zrzeszania się w związkach zawodowych, organizacjach społeczno-zawodowych rolników oraz w organizacjach pracodawców. 2. Związki zawodowe oraz pracodawcy i ich organizacje mają prawo do rokowań, w szczególności w celu rozwiązywania sporów zbiorowych, oraz do zawierania układów zbiorowych pracy i innych porozumień. 3. Związkom zawodowym przysługuje prawo do organizowania strajków pracowniczych i innych form protestu w granicach określonych w ustawie. Ze względu na dobro publiczne ustawa może ograniczyć prowadzenie strajku lub zakazać go w odniesieniu do określonych kategorii pracowników lub w określonych dziedzinach. 4. Zakres wolności zrzeszania się w związkach zawodowych i organizacjach pracodawców oraz innych wolności związkowych może podlegać tylko takim ograniczeniom ustawowym, jakie są dopuszczalne przez wiążące Rzeczpospolitą Polską umowy międzynarodowe.
Art. 12 Karty Praw Podstawowych Unii Europejskiej	1. Każdy ma prawo do swobodnego, pokojowego zgromadzania się oraz do swobodnego stowarzyszania się na wszystkich poziomach, zwłaszcza w sprawach politycznych, związkowych i obywatelskich, z którego wynika prawo każdego do tworzenia związków zawodowych i przystępowania do nich dla obrony swoich interesów. 2. Partie polityczne na poziomie Unii przyczyniają się do wyrażania woli politycznej jej obywateli.
Art. 11 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	1. Każdy ma prawo do swobodnego, pokojowego zgromadzenia się oraz do swobodnego stowarzyszania się, włącznie z prawem tworzenia związków zawodowych i przystępowania do nich dla ochrony swoich interesów. 2. Wykonywanie tych praw nie może podlegać innym ograniczeniom niż te, które określa ustawa i które są konieczne w społeczeństwie demokratycznym z uwagi na interesy bezpieczeństwa państwowego lub publicznego, ochronę porządku i zapobieganie przestępstwu, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób. Niniejszy przepis nie stanowi przeszkody w nakładaniu zgodnych z prawem ograniczeń korzystania z tych praw przez członków sił zbrojnych, policji lub administracji państwowej.

- Prawem do zakazu ponownego sądzenia lub karania, które znalazło odwzorowanie w art. 50 KPP UE (Zakaz ponownego sądzenia lub karania w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary), w art. 4 Protokołu nr 7 do EKPC (Zakaz ponownego sądzenia lub karania) oraz pośrednio w art. 42 KRP, art. 45 KRP.

Art. 50 Karty Praw Podstawowych Unii Europejskiej	Nikt nie może być ponownie sądzony lub ukarany w postępowaniu karnym za ten sam czyn zabroniony pod groźbą kary, w odniesieniu do którego zgodnie z ustawą został już uprzednio uniewinniony lub za który został już uprzednio skazany prawomocnym wyrokiem na terytorium Unii.
Art. 4 Protokołu nr 7 do Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	1. Nikt nie może być ponownie sądzony lub ukarany w postępowaniu przed sądem tego samego Państwa za przestępstwo, za które został uprzednio skazany prawomocnym wyrokiem lub uniewinniony zgodnie z ustawą i zasadami postępowania karnego tego Państwa. 2. Postanowienia poprzedniego ustępu nie stoją na przeszkodzie wznowieniu postępowania zgodnie z ustawą i zasadami postępowania karnego danego Państwa, jeśli wyjdą na jaw nowo odkryte fakty lub jeśli w poprzednim postępowaniu popełniono poważną pomyłkę, która mogła mieć wpływ na wynik sprawy. 3. Żadne z postanowień niniejszego artykułu nie może być uchylone na podstawie artykułu 15 Konwencji (Uchylenie stosowania zobowiązań w stanie niebezpieczeństwa publicznego)[386].

[386] Art. 15 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności:

1. W przypadku wojny lub innego niebezpieczeństwa publicznego zagrażającego życiu narodu, każda z Wysokich Układających się Stron może podjąć środki uchylające stosowanie

Art. 42 Konstytucji Rzeczypospolitej Polskiej	1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu.
Art. 45 Konstytucji Rzeczypospolitej Polskiej	1. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki przez właściwy, niezależny, bezstronny i niezawisły sąd. 2. Wyłączenie jawności rozprawy może nastąpić ze względu na moralność, bezpieczeństwo państwa i porządek publiczny oraz ze względu na ochronę życia prywatnego stron lub inny ważny interes prywatny. Wyrok ogłaszany jest publicznie.

- Prawem do odszkodowania za bezprawne skazanie, które znalazło swoje odwzorowanie w art. 3 Protokołu nr 7 do EKPC (Odszkodowanie za bezprawne skazanie).

Art. 4 Protokołu nr 7 do Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	Każdemu skazanemu prawomocnie za przestępstwo, który odbył karę w wyniku takiego skazania, a następnie został uniewinniony lub ułaskawiony na tej podstawie, że nowy lub nowo ujawniony fakt dowiódł, iż nastąpiła pomyłka sądowa, przysługuje odszkodowanie zgodnie z ustawą lub praktyką w danym Państwie, jeżeli nie udowodniono, że jest on całkowicie lub częściowo odpowiedzialny za nieujawnienie faktu we właściwym czasie.

- Prawem do odwołania w sprawach karnych, które znalazło swoje odwzorowanie w art. 47 KPP UE (Prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu) oraz w art. 2 Protokołu nr 7 do EKPC (Prawo do odwołania w sprawach karnych) oraz pośrednio w art. 42 KRP oraz art. 45 KRP.

---

zobowiązań wynikających z niniejszej Konwencji w zakresie ściśle odpowiadającym wymogom sytuacji, pod warunkiem, że środki te nie są sprzeczne z innymi zobowiązaniami wynikającymi z prawa międzynarodowego.

2. Na podstawie powyższego przepisu nie można uchylić zobowiązań wynikających z artykułu 2, z wyjątkiem przypadków śmierci będących wynikiem zgodnych z prawem działań wojennych oraz zobowiązań zawartych w artykułach 3, 4 (ustęp 1) i 7.

3. Każda z Wysokich Układających się Stron korzystając z prawa do uchylenia zobowiązań poinformuje wyczerpująco Sekretarza Generalnego Rady Europy o środkach, które podjęła oraz powodach ich zastosowania. Informować będzie również Sekretarza Generalnego Rady Europy, kiedy podjęte środki przestaną działać, a przepisy Konwencji będą ponownie w pełni stosowane.

Art. 47 Karty Praw Podstawowych Unii Europejskiej	Każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w niniejszym artykule. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony uprzednio na mocy ustawy. Każdy ma możliwość uzyskania porady prawnej, skorzystania z pomocy obrońcy i przedstawiciela. Pomoc prawna jest udzielana osobom, które nie posiadają wystarczających środków, w zakresie, w jakim jest ona konieczna dla zapewnienia skutecznego dostępu do wymiaru sprawiedliwości.
Art. 2 Protokołu nr 7 do Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	1. Każdy, kto został uznany przez sąd za winnego popełnienia przestępstwa, ma prawo do rozpatrzenia przez sąd wyższej instancji jego sprawy, tak w przedmiocie orzeczenia o winie, jak i co do kary. Korzystanie z tego prawa, a także jego podstawy, reguluje ustawa. 2. Wyjątki od tego prawa mogą być stosowane w przypadku drobnych przestępstw, określonych w ustawie, lub w przypadkach, gdy dana osoba była sądzona w pierwszej instancji przez Sąd Najwyższy albo została uznana za winną i skazana w wyniku zaskarżenia wyroku uniewinniającego sądu pierwszej instancji.
Art. 42 Konstytucji Rzeczypospolitej Polskiej	1. Odpowiedzialności karnej podlega ten tylko, kto dopuścił się czynu zabronionego pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia. Zasada ta nie stoi na przeszkodzie ukaraniu za czyn, który w czasie jego popełnienia stanowił przestępstwo w myśl prawa międzynarodowego. 2. Każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. 3. Każdego uważa się za niewinnego, dopóki jego wina nie zostanie stwierdzona prawomocnym wyrokiem sądu.
Art. 45 Konstytucji Rzeczypospolitej Polskiej	1. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki przez właściwy, niezależny, bezstronny i niezawisły sąd. 2. Wyłączenie jawności rozprawy może nastąpić ze względu na moralność, bezpieczeństwo państwa i porządek publiczny oraz ze względu na ochronę życia prywatnego stron lub inny ważny interes prywatny. Wyrok ogłaszany jest publicznie.

- Prawem do własności, które znalazło swoje odwzorowanie w art. 64 KRP, art. 17 KPP UE (Prawo własności) oraz art. 1 Protokołu dodatkowego do EKPC (Ochrona własności).

Art. 64 Konstytucji Rzeczypospolitej Polskiej	1. Każdy ma prawo do własności, innych praw majątkowych oraz prawo dziedziczenia. 2. Własność, inne prawa majątkowe oraz prawo dziedziczenia podlegają równej dla wszystkich ochronie prawnej. 3. Własność może być ograniczona tylko w drodze ustawy i tylko w zakresie, w jakim nie narusza ona istoty prawa własności.
Art. 17 Karty Praw Podstawowych Unii Europejskiej	1. Każdy ma prawo do władania, używania, rozporządzania i przekazania w drodze spadku mienia nabytego zgodnie z prawem. Nikt nie może być pozbawiony swojej własności, chyba że w interesie publicznym, w przypadkach i na warunkach przewidzianych w ustawie, za słusznym odszkodowaniem za jej utratę wypłaconym we właściwym terminie. Korzystanie z mienia może podlegać regulacji ustawowej w zakresie, w jakim jest to konieczne ze względu na interes ogólny. 2. Własność intelektualna podlega ochronie.

Art. 1 Protokołu dodatkowego do Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności	Każda osoba fizyczna i prawna ma prawo do poszanowania swego mienia. Nikt nie może być pozbawiony swojej własności, chyba że w interesie publicznym i na warunkach przewidzianych przez ustawę oraz zgodnie z podstawowymi zasadami prawa międzynarodowego. Powyższe postanowienia nie będą jednak w żaden sposób naruszać prawa Państwa do wydawania takich ustaw, jakie uzna za konieczne dla uregulowania sposobu korzystania z własności zgodnie z interesem powszechnym lub w celu zapewnienia uiszczania podatków bądź innych należności lub kar pieniężnych[387].

9.2. Metodologia

Podczas prac badawczych wykorzystano potencjał i możliwości, jakie daje klasyczna dla nauk prawnych metoda dogmatyczno-formalna (zawierająca elementy egzegezy treści aktu prawnego oraz hermeneutyki językowej). Na uwagę zasługuje także fakt wykorzystania metody prawnoporównawczej. W jej ramach posłużono się metodą komparatystyki prawniczej Kötza i Zweigerta. Składa się ona z pięciu faz, które mogą stanowić określony plan działania. Zgodnie z nimi następują po sobie: a) sformułowanie problemu; b) wybór materiału do porównania; c) właściwe porównanie; d) budowanie systemu uwzględniającego rezultaty porównania w praktyce; e) krytyczna ocena wyników osiągniętych poprzez porównanie[388]. Do instrumentarium badawczego należały także inne metody: heurystyczne (odroczone wartościowanie, transpozycja, sugerowanie oraz metody złożone), funkcjonalne (hermeneutyka swobodna), analizy i krytyki piśmiennictwa, analizy i konstrukcji logicznej, badania dokumentów, monograficzne oraz obserwacyjne. Dodatkowo, badacze dokonujący analiz wzięli pod uwagę metajęzykowo określony wskaźnik wpływu (liczba wypracowanych rozwiązań włączonych do głównego nurtu polityki; liczba wdrożonych strategii, dokumentów operacyjnych i konkretnych rozwiązań; liczba instytucji korzystających z wypracowanych rozwiązań; liczba osób korzystających z wypracowanych rozwiązań) i/albo wskaźnik rezultatu (liczba zakończonych pilotaży (wdrożeń) wypracowanych

[387] Należy pamiętać, że specyfika zakresu przedmiotowego i prawidłowej wykładni wskazanych powyżej norm ochrony praw człowieka wyznaczana jest przez orzecznictwo, odpowiednio: Trybunału Sprawiedliwości Unii Europejskiej oraz Europejskiego Trybunału Praw Człowieka.

[388] Zob. *Polska komparatystyka prawa. Prawo obce w doktrynie prawa polskiego*, red. A. Wudarski, Warszawa 2016; R. Tokarczyk, *Komparatystyka prawnicza*, Warszawa 2008.

rozwiązań; liczba osób zaangażowanych w wypracowanie rozwiązań; liczba publikacji, w tym publikacji internetowych, na temat wypracowanych rozwiązań) i/albo wskaźnik produktu (liczba wypracowanych diagnoz; liczba wypracowanych polityk, strategii oraz dokumentów operacyjnych; liczba opracowanych rozwiązań; liczba pilotaży (wdrożeń) wypracowanych rozwiązań).

9.3. Analiza *de lege lata* przestępstw finansowych w Polsce

9.3.1. Wstęp

Celem naukowym przedmiotowego podrozdziału jest analiza typów czynów zabronionych występujących w Polce, a dotyczących szeroko rozumianego rynku finansowego. Powyższe uzasadnione jest z metodologicznego oraz logicznego punktu widzenia. Dzieje się tak dlatego, że nawet najbardziej teoretyczne opracowania nie mogą abstrahować od rzeczywistego i aktualnego stanu prawnego. Dodatkowo podkreślenia wymaga fakt, że niniejsze opracowanie nie posiada jedynie walorów czysto teoretycznych, lecz poruszono w nim również praktyczne aspekty przeciwdziałania przyczynom przestępczości na rynku finansowym. W związku z powyższym celowe jest zaprezentowanie najważniejszych aktów prawnych obowiązujących powszechnie w Polsce zawierających zakazane zachowania o znamionach korelujących z szeroko rozumianym rynkiem finansowym.

9.3.2. Kodeks karny skarbowy

Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy[389] stanowi główny akt prawny zawierający katalog typów czynów zabronionych w zakresie przestępczości finansowej w sektorze publicznym. W zakresie prawa materialnego kodeks składa się z dwóch części: ogólnej oraz szczególnej. W pierwszej z nich zawarto przepisy określające zasady odpowiedzialności karnej skarbowej,

[389] Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (t.j. Dz.U. z 2018 r., poz. 1958, 2192, 2193, 2227, 2354).

zaniechania ukarania sprawcy, przestępstwa skarbowe (normy ogólne mające zastosowanie do konkretnych typów czynów zabronionych stypizowanych w części szczególnej Kodeksu karnego skarbowego), wykroczenia skarbowe (normy ogólne mające zastosowanie do konkretnych typów czynów zabronionych stypizowanych w części szczególnej Kodeksu karnego skarbowego) oraz objaśnienia wyrażeń ustawowych. Natomiast w części szczególnej kodeksu zawarto przepisy określające przestępstwa skarbowe i wykroczenia skarbowe przeciwko obowiązkom podatkowym i rozliczeniom z tytułu dotacji lub subwencji (art. 54–84), przestępstwa skarbowe i wykroczenia skarbowe przeciwko obowiązkom celnym oraz zasadom obrotu z zagranicą towarami i usługami (art. 85–96), przestępstwa skarbowe i wykroczenia skarbowe przeciwko obrotowi dewizowemu (art. 97–106ł), przestępstwa skarbowe i wykroczenia skarbowe przeciwko organizacji gier hazardowych (art. 107–111). Poniżej zaprezentowano najcięższe typy czynów zabronionych stypizowanych w Kodeksie karnym skarbowym, bowiem zgodnie z jego art. 27, jeżeli kodeks nie stanowi inaczej, kara pozbawienia wolności trwa najkrócej 5 dni, najdłużej – 5 lat. Zatem celowe jest zaprezentowanie tych typów przestępstw skarbowych, w których kodeks nie stanowi o innym (lżejszym, gdyż nie ma przypadku podniesienia przedmiotowej granicy) wymiarze kary.

Art. 54	§ 1. Podatnik, który uchylając się od opodatkowania, nie ujawnia właściwemu organowi przedmiotu lub podstawy opodatkowania lub nie składa deklaracji, przez co naraża podatek na uszczuplenie, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Jeżeli kwota podatku narażonego na uszczuplenie jest małej wartości, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny do 720 stawek dziennych. § 3. Jeżeli kwota podatku narażonego na uszczuplenie nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.
Art. 56	§ 1. Podatnik, który składając organowi podatkowemu, innemu uprawnionemu organowi lub płatnikowi deklarację lub oświadczenie, podaje nieprawdę lub zataja prawdę albo nie dopełnia obowiązku zawiadomienia o zmianie objętych nimi danych, przez co naraża podatek na uszczuplenie, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Jeżeli kwota podatku narażonego na uszczuplenie jest małej wartości, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny do 720 stawek dziennych. § 3. Jeżeli kwota podatku narażonego na uszczuplenie nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe. § 4. Karze określonej w § 3 podlega także ten podatnik, który mimo ujawnienia przedmiotu lub podstawy opodatkowania nie składa w terminie organowi podatkowemu lub płatnikowi deklaracji lub oświadczenia lub wbrew obowiązkowi nie składa ich za pomocą środków komunikacji elektronicznej.

Art. 56d	§ 1. Kto podaje nieprawdę lub zataja prawdę składając: 1) oświadczenie, o którym mowa w **art. 41** ust. 15, 21 lub 25 ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych lub w **art. 26** ust. 1ab, 7a lub 7g ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych, 2) oświadczenie co do zgodności z prawdą faktów przedstawionych we wniosku o zwrot podatku, o którym mowa w rozdziale 7b ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych lub w rozdziale 6a ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych lub we wniosku o wydanie opinii o stosowaniu zwolnienia, o którym mowa w **art. 26b** ust. 1 ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych, oraz co do zgodności z oryginałem dokumentacji załączonej do tych wniosków, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 3. W wypadku mniejszej wagi, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.
Art. 57a	§ 1. Komornik sądowy, który wbrew obowiązkowi, o którym mowa w **art. 149** ust. 2 ustawy z dnia 22 marca 2018 r. o komornikach sądowych (Dz.U. poz. 771, 1443 i 1669), nie przekazuje na rachunek właściwego urzędu skarbowego podlegających przekazaniu opłat egzekucyjnych albo przekazuje je w niewłaściwej wysokości, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Jeżeli kwota należności, o których mowa w § 1, jest małej wartości, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny do 720 stawek dziennych. § 3. Jeżeli kwota należności, o których mowa w § 1, nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.
Art. 62	§ 1. Kto wbrew obowiązkowi nie wystawia faktury lub rachunku, wystawia je w sposób wadliwy albo odmawia ich wydania, podlega karze grzywny do 180 stawek dziennych. § 2. Kto fakturę lub rachunek wystawia w sposób nierzetelny albo takim dokumentem się posługuje, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności na czas nie krótszy od roku, albo obu tym karom łącznie. § 3. a. Kto fakturę lub rachunek wystawia w sposób nierzetelny albo takim dokumentem się posługuje, a kwota podatku wynikająca z faktury albo suma kwot podatku wynikających z faktur jest małej wartości, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 4. Karze określonej w § 1 podlega także ten, kto wbrew obowiązkowi nie przechowuje wystawionej lub otrzymanej faktury lub rachunku, bądź dowodu zakupu towarów. § 5. Karze określonej w § 1 podlega także ten, kto wbrew przepisom ustawy dokona sprzedaży z pominięciem kasy rejestrującej albo nie wyda dokumentu z kasy rejestrującej, stwierdzającego dokonanie sprzedaży. § 6. W wypadku mniejszej wagi, sprawca czynu zabronionego określonego w § 1–4 podlega karze grzywny za wykroczenie skarbowe.
Art. 67	§ 1. Kto podrabia albo przerabia znak akcyzy albo upoważnienie do odbioru banderol, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Kto w celu popełnienia przestępstwa skarbowego określonego w § 1 uzyskuje lub przysposabia środki, podlega karze grzywny do 240 stawek dziennych albo karze pozbawienia wolności do lat 2, albo obu tym karom łącznie. § 3. Nie podlega karze za przestępstwo skarbowe określone w § 2 sprawca, który odstąpił od jego dokonania, w szczególności zniszczył uzyskane lub przysposobione środki lub zapobiegł skorzystaniu z nich w przyszłości. § 4. W wypadku mniejszej wagi, sprawca czynu zabronionego określonego w § 1 lub 2 podlega karze grzywny za wykroczenie skarbowe.
Art. 69b	§ 1. Kto wbrew przepisom ustawy dokonuje dostawy wewnątrzwspólnotowej lub nabycia wewnątrzwspólnotowego wyrobów akcyzowych, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. W wypadku mniejszej wagi, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.

Art. 69c	§ 1. Kto wbrew obowiązkowi przemieszcza wyroby akcyzowe z terytorium jednego państwa członkowskiego na terytorium innego państwa członkowskiego przez terytorium kraju bez uproszczonego dokumentu towarzyszącego albo dokumentu handlowego zastępującego uproszczony dokument towarzyszący albo bez wydruku e-AD z nadanym numerem referencyjnym albo innego dokumentu handlowego, w którym umieszczono numer referencyjny nadany e-AD w Systemie, albo dokumentu zastępującego e-AD, albo na podstawie tych dokumentów zawierających dane niezgodne ze stanem rzeczywistym, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. W wypadku mniejszej wagi, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.
Art. 76	§ 1. Kto przez podanie danych niezgodnych ze stanem rzeczywistym lub zatajenie rzeczywistego stanu rzeczy wprowadza w błąd właściwy organ narażając na nienależny zwrot podatkowej należności publiczno-prawnej, w szczególności podatku naliczonego w rozumieniu przepisów o podatku od towarów i usług, podatku akcyzowym, zwrot nadpłaty lub jej zaliczenie na poczet zaległości podatkowej lub bieżących albo przyszłych zobowiązań podatkowych, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Jeżeli kwota narażona na nienależny zwrot podatku jest małej wartości, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny do 720 stawek dziennych. § 3. Jeżeli kwota narażona na nienależny zwrot podatku nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.
Art. 76a	§ 1. Kto przez podanie danych niezgodnych ze stanem rzeczywistym lub zatajenie rzeczywistego stanu rzeczy wprowadza w błąd właściwy organ narażając na nienależny zwrot wydatków, o których mowa w przepisach o zwrocie osobom fizycznym niektórych wydatków związanych z budownictwem mieszkaniowym, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Jeżeli kwota narażona na nienależny zwrot wydatków, o których mowa w § 1, jest małej wartości, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny do 720 stawek dziennych. § 3. Jeżeli kwota narażona na nienależny zwrot wydatków, o których mowa w § 1, nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.
Art. 76b	§1. Kto przez podanie danych niezgodnych ze stanem rzeczywistym lub zatajenie rzeczywistego stanu rzeczy wprowadza w błąd właściwy organ narażając na nienależny zwrot wydatków, o których mowa w przepisach o zwrocie osobom fizycznym niektórych wydatków poniesionych w związku z budową pierwszego własnego mieszkania, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. §2. Jeżeli kwota narażona na nienależny zwrot wydatków, o których mowa w § 1, jest małej wartości, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny do 720 stawek dziennych. §3. Jeżeli kwota narażona na nienależny zwrot wydatków, o których mowa w § 1, nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.
Art. 86	§ 1. Kto, nie dopełniając ciążącego na nim obowiązku celnego, przywozi z zagranicy lub wywozi za granicę towar bez jego przedstawienia organowi celnemu lub zgłoszenia celnego, przez co naraża należność celną na uszczuplenie, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Tej samej karze podlega sprawca, jeżeli przemyt celny dotyczy towaru w obrocie z zagranicą, co do którego istnieje reglamentacja pozataryfowa. § 3. Jeżeli kwota należności celnej narażonej na uszczuplenie lub wartość towaru w obrocie z zagranicą, co do którego istnieje reglamentacja pozataryfowa, jest małej wartości, sprawca czynu zabronionego określonego w § 1 lub 2 podlega karze grzywny do 720 stawek dziennych. § 4. Jeżeli kwota należności celnej narażonej na uszczuplenie lub wartość towaru w obrocie z zagranicą, co do którego istnieje reglamentacja pozataryfowa, nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 lub 2 podlega karze grzywny za wykroczenie skarbowe. § 5. (uchylony)

Art. 87	§ 1. Kto przez wprowadzenie w błąd organu uprawnionego do kontroli celnej naraża należność celną na uszczuplenie, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Tej samej karze podlega sprawca, jeżeli oszustwo celne dotyczy towaru lub usługi w obrocie z zagranicą, co do których istnieje reglamentacja pozataryfowa. § 3. Jeżeli kwota należności celnej narażonej na uszczuplenie lub wartość towaru lub usługi w obrocie z zagranicą, co do których istnieje reglamentacja pozataryfowa, jest małej wartości, sprawca czynu zabronionego określonego w § 1 lub 2 podlega karze grzywny do 720 stawek dziennych. § 4. Jeżeli kwota należności celnej narażonej na uszczuplenie lub wartość towaru lub usługi w obrocie z zagranicą, co do których istnieje reglamentacja pozataryfowa, nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 lub 2 podlega karze grzywny za wykroczenie skarbowe.
Art. 92	§ 1. Kto przez podanie danych niezgodnych ze stanem rzeczywistym lub zatajenie rzeczywistego stanu rzeczy wprowadza w błąd właściwy organ narażając na nienależny zwrot należności celnej lub umorzenie należności celnej należnej do zapłacenia, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 2. Jeżeli kwota narażona na nienależny zwrot lub umorzenie należności celnej jest małej wartości, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny do 720 stawek dziennych. § 3. Jeżeli kwota narażona na nienależny zwrot lub umorzenie należności celnej nie przekracza ustawowego progu, sprawca czynu zabronionego określonego w § 1 podlega karze grzywny za wykroczenie skarbowe.
Art. 107	§ 1. Kto wbrew przepisom ustawy lub warunkom koncesji lub zezwolenia urządza lub prowadzi gry hazardowe, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności do lat 3, albo obu tym karom łącznie. § 2. Kto na terytorium Rzeczypospolitej Polskiej uczestniczy w zagranicznej grze hazardowej, podlega karze grzywny do 120 stawek dziennych. § 3. Jeżeli sprawca dopuszcza się czynu zabronionego określonego w § 1 w celu osiągnięcia korzyści majątkowej z organizowania zbiorowego uczestnictwa w grze hazardowej, podlega karze grzywny do 720 stawek dziennych albo karze pozbawienia wolności, albo obu tym karom łącznie. § 4. W wypadku mniejszej wagi, sprawca czynu zabronionego określonego w § 1 lub 2 podlega karze grzywny za wykroczenie skarbowe.

9.4. Kodeks karny

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny[390] stanowi główny akt prawa karnego materialnego w polskim porządku normatywnym. Składa się ona z dwóch części: ogólnej oraz szczególnej. Pierwsza z nich zawiera zasady odpowiedzialności karnej (art. 1–12), formy popełnienia przestępstwa (art. 13–24), wyłączenie odpowiedzialności karnej (art. 25–31), kary (art. 32–38), środki karne (art. 39–43c), przepadek i środki kompensacyjne (art. 44–52), zasady wymiaru kary i środków karnych (art. 53–63), powrót do przestępstwa (art. 64–65), środki związane z poddaniem sprawcy próbie (art. 66–84a), zbieg przestępstw oraz łączenie kar środków karnych (art. 85–92a), środki zabezpieczające (art. 93–100), przedawnienie (art. 101–105), zatarcie skazania

[390] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2018 r., poz. 1600 z późn. zm.).

(art. 106–108), odpowiedzialność za przestępstwa popełnione za granicą (art. 109–114a), objaśnienie wyrażeń ustawowych (art. 115) oraz stosunek do ustaw szczegółowych (art. 116). Druga z nich składa się ze stypizowanych typów czynów zabronionych, które ułożone zostały ze względu na rodzaj dobra prawnego podlegającego ochronie prawnej. Rodzaj dobra prawnego podlegającego prawnokarnej ochronie zależy od powszechnie zaakceptowanych wartości przez konkretne społeczeństwo, które następczo zostają określone w ustawie karnej. Aktualnie obowiązujący Kodeks karny w Polsce wyróżnia następujące typy dóbr prawnych, które chroni pod groźbą kary w postaci:

- Przestępstw przeciwko pokojowi, ludzkości oraz przestępstwa wojenne (art. 117–126c);
- Przestępstw przeciwko Rzeczypospolitej Polskiej (art. 127–139);
- Przestępstw przeciwko obronności (art. 140–147);
- Przestępstw przeciwko życiu i zdrowiu (art. 148–162);
- Przestępstw przeciwko bezpieczeństwu powszechnemu (art. 163–172);
- Przestępstw przeciwko bezpieczeństwu w komunikacji (art. 173–180a);
- Przestępstw przeciwko środowisku (art. 181–188);
- Przestępstw przeciwko wolności (art. 189–193);
- Przestępstw przeciwko wolności sumienia i wyznania (art. 194–196);
- Przestępstw przeciwko wolności seksualnej i obyczajności (197–205);
- Przestępstw przeciwko rodzinie i opiece (art. 206–211a);
- Przestępstw przeciwko czci i nietykalności cielesnej (art. 212–217a);
- Przestępstw przeciwko prawom osób wykonujących pracę zarobkową (art. 218–221);
- Przestępstw przeciwko działalności instytucji państwowych oraz samorządu terytorialnego (art. 222–231b);
- Przestępstw przeciwko wymiarowi sprawiedliwości (art. 232–247a);
- Przestępstw przeciwko wyborom i referendum (art. 248–251);
- Przestępstw przeciwko porządkowi publicznemu (art. 252–264a);
- Przestępstw przeciwko ochronie informacji (art. 265–269c);
- Przestępstw przeciwko wiarygodności dokumentów (art. 270–277d);
- Przestępstw przeciwko mieniu (art. 278–295);
- Przestępstw przeciwko obrotowi gospodarczemu (art. 296–309);

- Przestępstw przeciwko obrotowi pieniędzmi i papierami wartościowymi (art. 310–316).

Okazuje się, że przepisy Kodeksu karnego mają duże znaczenie dla badanej materii. Dzieje się tak dlatego, że wśród dóbr prawnych podlegających prawnokarnej ochronie znalazły się też takie jak obrót gospodarczy, pieniędzmi oraz papierami wartościowymi. Poniżej zaprezentowano typy czynów zabronionych, które bezpośrednio odnoszą się do szeroko rozumianego rynku finansowego.

Art. 231	§ 1. Funkcjonariusz publiczny[391], który, przekraczając swoje uprawnienia lub nie dopełniając obowiązków, działa na szkodę interesu publicznego lub prywatnego, podlega karze pozbawienia wolności do lat 3. § 2. Jeżeli sprawca dopuszcza się czynu określonego w § 1 w celu osiągnięcia korzyści majątkowej lub osobistej, podlega karze pozbawienia wolności od roku do lat 10. § 3. Jeżeli sprawca czynu określonego w § 1 działa nieumyślnie i wyrządza istotną szkodę, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 4. Przepisu § 2 nie stosuje się, jeżeli czyn wyczerpuje znamiona czynu zabronionego określonego w **art. 228**
Art. 282	Kto, w celu osiągnięcia korzyści majątkowej, przemocą, groźbą zamachu na życie lub zdrowie albo gwałtownego zamachu na mienie, doprowadza inną osobę do rozporządzenia mieniem własnym lub cudzym albo do zaprzestania działalności gospodarczej, podlega karze pozbawienia wolności od roku do lat 10.
Art. 286	§ 1. Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 2. Tej samej karze podlega, kto żąda korzyści majątkowej w zamian za zwrot bezprawnie zabranej rzeczy. § 3. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 4. Jeżeli czyn określony w § 1–3 popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

[391] Zgodnie z art. 115 § 13 funkcjonariuszem publicznym jest: 1) Prezydent Rzeczypospolitej Polskiej; 2) poseł, senator, radny; 2a) poseł do Parlamentu Europejskiego; 3) sędzia, ławnik, prokurator, funkcjonariusz finansowego organu postępowania przygotowawczego lub organu nadrzędnego nad finansowym organem postępowania przygotowawczego, notariusz, komornik, kurator sądowy, syndyk, nadzorca sądowy i zarządca, osoba orzekająca w organach dyscyplinarnych działających na podstawie ustawy; 4) osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych; 5) osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe; 6) osoba zajmująca kierownicze stanowisko w innej instytucji państwowej; 7) funkcjonariusz organu powołanego do ochrony bezpieczeństwa publicznego albo funkcjonariusz Służby Więziennej; 8) osoba pełniąca czynną służbę wojskową, z wyjątkiem terytorialnej służby wojskowej pełnionej dyspozycyjnie; 9) pracownik międzynarodowego trybunału karnego, chyba że pełni wyłącznie czynności usługowe.

Art. 287	§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. § 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.
Art. 296	§ 1. Kto, będąc obowiązany na podstawie przepisu ustawy, decyzji właściwego organu lub umowy do zajmowania się sprawami majątkowymi lub działalnością gospodarczą osoby fizycznej, prawnej albo jednostki organizacyjnej niemającej osobowości prawnej, przez nadużycie udzielonych mu uprawnień lub niedopełnienie ciążącego na nim obowiązku, wyrządza jej znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 1a. Jeżeli sprawca, o którym mowa w § 1, przez nadużycie udzielonych mu uprawnień lub niedopełnienie ciążącego na nim obowiązku, sprowadza bezpośrednie niebezpieczeństwo wyrządzenia znacznej szkody majątkowej, podlega karze pozbawienia wolności do lat 3. § 2. Jeżeli sprawca przestępstwa określonego w § 1 lub 1a działa w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 3. Jeżeli sprawca przestępstwa określonego w § 1 lub 2 wyrządza szkodę majątkową w wielkich rozmiarach, podlega karze pozbawienia wolności od roku do lat 10. § 4. Jeżeli sprawca przestępstwa określonego w § 1 lub 3 działa nieumyślnie, podlega karze pozbawienia wolności do lat 3. § 4a. Jeżeli pokrzywdzonym nie jest Skarb Państwa, ściganie przestępstwa określonego w § 1a następuje na wniosek pokrzywdzonego. § 5. Nie podlega karze, kto przed wszczęciem postępowania karnego dobrowolnie naprawił w całości wyrządzoną szkodę.
Art. 296a	§ 1. Kto, pełniąc funkcję kierowniczą w jednostce organizacyjnej wykonującej działalność gospodarczą lub pozostając z nią w stosunku pracy, umowy zlecenia lub umowy o dzieło, żąda lub przyjmuje korzyść majątkową lub osobistą albo jej obietnicę, w zamian za nadużycie udzielonych mu uprawnień lub niedopełnienie ciążącego na nim obowiązku mogące wyrządzić tej jednostce szkodę majątkową albo stanowiące czyn nieuczciwej konkurencji lub niedopuszczalną czynność preferencyjną na rzecz nabywcy lub odbiorcy towaru, usługi lub świadczenia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 2. Tej samej karze podlega, kto w wypadkach określonych w § 1 udziela albo obiecuje udzielić korzyści majątkowej lub osobistej. § 3. W wypadku mniejszej wagi, sprawca czynu określonego w § 1 lub 2 podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 4. Jeżeli sprawca czynu określonego w § 1 wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 5. Nie podlega karze sprawca przestępstwa określonego w § 2 albo w § 3 w związku z § 2, jeżeli korzyść majątkowa lub osobista albo ich obietnica zostały przyjęte, a sprawca zawiadomił o tym fakcie organ powołany do ścigania przestępstw i ujawnił wszystkie istotne okoliczności przestępstwa, zanim organ ten o nim się dowiedział.

Art. 297	§ 1. Kto, w celu uzyskania dla siebie lub kogo innego, od banku lub jednostki organizacyjnej prowadzącej podobną działalność gospodarczą na podstawie ustawy albo od organu lub instytucji dysponujących środkami publicznymi – kredytu, pożyczki pieniężnej, poręczenia, gwarancji, akredytywy, dotacji, subwencji, potwierdzenia przez bank zobowiązania wynikającego z poręczenia lub z gwarancji lub podobnego świadczenia pieniężnego na określony cel gospodarczy, instrumentu płatniczego lub zamówienia publicznego, przedkłada podrobiony, przerobiony, poświadczający nieprawdę albo nierzetelny dokument albo nierzetelne, pisemne oświadczenie dotyczące okoliczności o istotnym znaczeniu dla uzyskania wymienionego wsparcia finansowego, instrumentu płatniczego lub zamówienia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 2. Tej samej karze podlega, kto wbrew ciążącemu obowiązkowi, nie powiadamia właściwego podmiotu o powstaniu sytuacji mogącej mieć wpływ na wstrzymanie albo ograniczenie wysokości udzielonego wsparcia finansowego, określonego w § 1, lub zamówienia publicznego albo na możliwość dalszego korzystania z instrumentu płatniczego. § 3. Nie podlega karze, kto przed wszczęciem postępowania karnego dobrowolnie zapobiegł wykorzystaniu wsparcia finansowego lub instrumentu płatniczego, określonych w § 1, zrezygnował z dotacji lub zamówienia publicznego albo zaspokoił roszczenia pokrzywdzonego.
Art. 298	§ 1. Kto, w celu uzyskania odszkodowania z tytułu umowy ubezpieczenia, powoduje zdarzenie będące podstawą do wypłaty takiego odszkodowania, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 2. Nie podlega karze, kto przed wszczęciem postępowania karnego dobrowolnie zapobiegł wypłacie odszkodowania.
Art. 299	§ 1. Kto środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości, pochodzące z korzyści związanych z popełnieniem czynu zabronionego, przyjmuje, posiada, używa, przekazuje lub wywozi za granicę, ukrywa, dokonuje ich transferu lub konwersji, pomaga do przenoszenia ich własności lub posiadania albo podejmuje inne czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie ich przestępnego pochodzenia lub miejsca umieszczenia, ich wykrycie, zajęcie albo orzeczenie przepadku, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 2. Karze określonej w § 1 podlega, kto będąc pracownikiem lub działając w imieniu lub na rzecz banku, instytucji finansowej lub kredytowej lub innego podmiotu, na którym na podstawie przepisów prawa ciąży obowiązek rejestracji transakcji i osób dokonujących transakcji, przyjmuje, wbrew przepisom, środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, dokonuje ich transferu lub konwersji, lub przyjmuje je w innych okolicznościach wzbudzających uzasadnione podejrzenie, że stanowią one przedmiot czynu określonego w § 1, lub świadczy inne usługi mające ukryć ich przestępne pochodzenie lub usługi w zabezpieczeniu przed zajęciem. § 3. (uchylony) § 4. (uchylony) § 5. Jeżeli sprawca dopuszcza się czynu określonego w § 1 lub 2, działając w porozumieniu z innymi osobami, podlega karze pozbawienia wolności od roku do lat 10. § 6. Karze określonej w § 5 podlega sprawca, jeżeli dopuszczając się czynu określonego w § 1 lub 2, osiąga znaczną korzyść majątkową. § 6a. Kto czyni przygotowania do przestępstwa określonego w § 1 lub 2, podlega karze pozbawienia wolności do lat 3. § 7. W razie skazania za przestępstwo określone w § 1 lub 2, sąd orzeka przepadek przedmiotów pochodzących bezpośrednio albo pośrednio z przestępstwa, a także korzyści z tego przestępstwa lub ich równowartość, chociażby nie stanowiły one własności sprawcy. Przepadku nie orzeka się w całości lub w części, jeżeli przedmiot, korzyść lub jej równowartość podlega zwrotowi pokrzywdzonemu lub innemu podmiotowi. § 8. Nie podlega karze za przestępstwo określone w § 1 lub 2, kto dobrowolnie ujawnił wobec organu powołanego do ścigania przestępstw informacje dotyczące osób uczestniczących w popełnieniu przestępstwa oraz okoliczności jego popełnienia, jeżeli zapobiegło to popełnieniu innego przestępstwa; jeżeli sprawca czynił starania zmierzające do ujawnienia tych informacji i okoliczności, sąd stosuje nadzwyczajne złagodzenie kary.

Art. 300	§ 1. Kto, w razie grożącej mu niewypłacalności lub upadłości, udaremnia lub uszczupla zaspokojenie swojego wierzyciela przez to, że usuwa, ukrywa, zbywa, darowuje, niszczy, rzeczywiście lub pozornie obciąża albo uszkadza składniki swojego majątku, podlega karze pozbawienia wolności do lat 3. § 2. Kto, w celu udaremnienia wykonania orzeczenia sądu lub innego organu państwowego, udaremnia lub uszczupla zaspokojenie swojego wierzyciela przez to, że usuwa, ukrywa, zbywa, darowuje, niszczy, rzeczywiście lub pozornie obciąża albo uszkadza składniki swojego majątku zajęte lub zagrożone zajęciem, bądź usuwa znaki zajęcia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 3. Jeżeli czyn określony w § 1 wyrządził szkodę wielu wierzycielom, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8. § 4. Jeżeli pokrzywdzonym nie jest Skarb Państwa, ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.
Art. 301	§ 1. Kto będąc dłużnikiem kilku wierzycieli udaremnia lub ogranicza zaspokojenie ich należności przez to, że tworzy w oparciu o przepisy prawa nową jednostkę gospodarczą i przenosi na nią składniki swojego majątku, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 2. Tej samej karze podlega, kto będąc dłużnikiem kilku wierzycieli doprowadza do swojej upadłości lub niewypłacalności. § 3. Kto będąc dłużnikiem kilku wierzycieli w sposób lekkomyślny doprowadza do swojej upadłości lub niewypłacalności, w szczególności przez trwonienie części składowych majątku, zaciąganie zobowiązań lub zawieranie transakcji oczywiście sprzecznych z zasadami gospodarowania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
Art. 302	§ 1. Kto, w razie grożącej mu niewypłacalności lub upadłości, nie mogąc zaspokoić wszystkich wierzycieli, spłaca lub zabezpiecza tylko niektórych, czym działa na szkodę pozostałych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Kto wierzycielowi udziela lub obiecuje udzielić korzyści majątkowej za działanie na szkodę innych wierzycieli w związku z postępowaniem upadłościowym lub zmierzającym do zapobiegnięcia upadłości, podlega karze pozbawienia wolności do lat 3. § 3. Tej samej karze podlega wierzyciel, który w związku z określonym w § 2 postępowaniem przyjmuje korzyść za działanie na szkodę innych wierzycieli albo takiej korzyści żąda.
Art. 303	§ 1. Kto wyrządza szkodę majątkową osobie fizycznej, prawnej lub jednostce organizacyjnej niemającej osobowości prawnej, przez nieprowadzenie dokumentacji działalności gospodarczej albo prowadzenie jej w sposób nierzetelny lub niezgodny z prawdą, w szczególności niszcząc, usuwając, ukrywając, przerabiając lub podrabiając dokumenty dotyczące tej działalności, podlega karze pozbawienia wolności do lat 3. § 2. Jeżeli sprawca przestępstwa określonego w § 1 wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 3. W wypadku mniejszej wagi, sprawca przestępstwa określonego w § 1 podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. § 4. Jeżeli pokrzywdzonym nie jest Skarb Państwa, ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.
Art. 304	Kto, wyzyskując przymusowe położenie innej osoby fizycznej, prawnej albo jednostki organizacyjnej niemającej osobowości prawnej, zawiera z nią umowę, nakładając na nią obowiązek świadczenia niewspółmiernego ze świadczeniem wzajemnym, podlega karze pozbawienia wolności do lat 3.
Art. 305	§ 1. Kto, w celu osiągnięcia korzyści majątkowej, udaremnia lub utrudnia przetarg publiczny albo wchodzi w porozumienie z inną osobą działając na szkodę właściciela mienia albo osoby lub instytucji, na rzecz której przetarg jest dokonywany, podlega karze pozbawienia wolności do lat 3. § 2. Tej samej karze podlega, kto w związku z publicznym przetargiem rozpowszechnia informacje lub przemilcza istotne okoliczności mające znaczenie dla zawarcia umowy będącej przedmiotem przetargu albo wchodzi w porozumienie z inną osobą, działając na szkodę właściciela mienia albo osoby lub instytucji, na rzecz której przetarg jest dokonywany. § 3. Jeżeli pokrzywdzonym nie jest Skarb Państwa, ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.
Art. 306	Kto usuwa, podrabia lub przerabia znaki identyfikacyjne, datę produkcji lub datę przydatności towaru lub urządzenia, podlega karze pozbawienia wolności do lat 3.

Art. 310	§ 1. Kto podrabia lub przerabia polski albo obcy pieniądz, polski albo obcy znak pieniężny, który został ustalony jako prawny środek płatniczy, jednak nie został jeszcze wprowadzony do obiegu, inny środek płatniczy albo dokument uprawniający do otrzymania sumy pieniężnej albo zawierający obowiązek wypłaty kapitału, odsetek, udziału w zyskach albo stwierdzenie uczestnictwa w spółce lub z pieniędzy, innego środka płatniczego albo z takiego dokumentu usuwa oznakę umorzenia, podlega karze pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności. § 2. Kto pieniądz, inny środek płatniczy lub znak pieniężny albo dokument określone w § 1 puszcza w obieg albo go w takim celu przyjmuje, przechowuje, przewozi, przenosi, przesyła albo pomaga do jego zbycia lub ukrycia, podlega karze pozbawienia wolności od roku do lat 10. § 3. W wypadku mniejszej wagi sąd może zastosować nadzwyczajne złagodzenie kary. § 4. Kto czyni przygotowania do popełnienia przestępstwa określonego w § 1 lub 2, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
Art. 311.	Kto, w dokumentacji związanej z obrotem papierami wartościowymi, rozpowszechnia nieprawdziwe informacje lub przemilcza informacje o stanie majątkowym oferenta, mające istotne znaczenie dla nabycia, zbycia papierów wartościowych, podwyższenia albo obniżenia wkładu, podlega karze pozbawienia wolności do lat 3.
Art. 312.	Kto puszcza w obieg podrobiony albo przerobiony pieniądz, inny środek płatniczy albo dokument określony w **art. 310** § 1, który sam otrzymał jako prawdziwy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
Art. 313	§ 1. Kto, w celu użycia lub puszczenia w obieg, podrabia albo przerabia urzędowy znak wartościowy albo ze znaku takiego usuwa oznakę umorzenia, podlega karze pozbawienia wolności do lat 3. § 2. Tej samej karze podlega, kto urzędowy znak wartościowy podrobiony, przerobiony albo z usuniętą oznaką umorzenia puszcza w obieg, nabywa lub go używa albo przechowuje w celu puszczenia w obieg.
Art. 314	Kto, w celu użycia w obrocie gospodarczym, podrabia lub przerabia znak urzędowy, mający stwierdzić upoważnienie lub wynik badania albo w obrocie publicznym używa przedmiotów opatrzonych takimi podrobionymi albo przerobionymi znakami, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
Art. 315	§ 1. Kto, w celu użycia w obrocie gospodarczym, podrabia lub przerabia zalegalizowane narzędzie pomiarowe lub probiercze, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Tej samej karze podlega, kto podrobionego albo przerobionego narzędzia pomiarowego lub probierczego w obrocie gospodarczym używa albo takie narzędzie w celu użycia w obrocie gospodarczym przechowuje.

9.5. Kodeks spółek handlowych

Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych[392] stanowi główny akt prawa gospodarczego prywatnego w Polsce. Określa ona tworzenie, organizację, funkcjonowanie, rozwiązywanie, łączenie, podział i przekształcanie spółek handlowych, a więc, co do zasady, spółek osobowych i kapitałowych. Choć zdecydowana część przepisów Kodeksu spółek handlowych należy do dziedziny prawa prywatnego, a nie publicznego, to znajdują się w nim także określone typy czynów zabronionych w kontekście regulowanej

[392] Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (t.j. Dz.U. 2019, poz. 505).

materii. Omawiana ustawa składa się z przepisów: ogólnych (art. 1–21), spółek osobowych (art. 22–150), spółek kapitałowych (art. 151–490), dotyczących łączenia, podziału i przekształcania spółek (art. 491–58413), karnych (art. 585–595) i dotyczących zmiany w przepisach obowiązujących oraz przejściowych i końcowych (art. 596–633). W związku z powyższym uzasadnione jest zaprezentowanie przepisów karnych Kodeksu spółek handlowych jako tych należących do obszaru rynku finansowego.

Art. 585	(uchylony)
Art. 586	Kto, będąc członkiem zarządu spółki albo likwidatorem, nie zgłasza wniosku o upadłość spółki handlowej pomimo powstania warunków uzasadniających według przepisów upadłość spółki – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
Art. 587	§ 1. Kto przy wykonywaniu obowiązków wymienionych w tytule III i IV ogłasza dane nieprawdziwe albo przedstawia je organom spółki, władzom państwowym lub osobie powołanej do rewizji – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Jeżeli sprawca działa nieumyślnie – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
Art. 588	Kto, będąc członkiem zarządu albo likwidatorem, dopuszcza do nabycia przez spółkę handlową własnych udziałów lub akcji albo do brania ich w zastaw – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do 6 miesięcy.
Art. 589	Kto, będąc członkiem zarządu albo likwidatorem spółki z ograniczoną odpowiedzialnością, dopuszcza do wydania przez spółkę dokumentów imiennych, na okaziciela lub dokumentów na zlecenie na udziały lub prawa do zysków w spółce – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do 6 miesięcy.
Art. 590	Kto w celu umożliwienia bezprawnego głosowania na walnym zgromadzeniu lub bezprawnego wykonywania praw mniejszości: 3) wystawia fałszywe zaświadczenie o złożeniu dokumentu akcji uprawniającej do głosowania, 4) użycza innemu dokumentu akcji, która nie uprawnia jej właściciela do głosowania, 5) wystawia fałszywe zaświadczenie o prawie uczestnictwa w walnym zgromadzeniu spółki publicznej, 6) przekazuje lub udostępnia fałszywy wykaz akcjonariuszy uprawnionych do uczestnictwa w walnym zgromadzeniu spółki publicznej – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
Art. 591	Kto przy głosowaniu na walnym zgromadzeniu lub wykonywaniu praw mniejszości posługuje się: 1) fałszywym zaświadczeniem o złożeniu dokumentu akcji uprawniającej do głosowania, 2) cudzym dokumentem akcji bez zgody właściciela, 3) cudzym dokumentem akcji, która nie uprawnia jej właściciela do głosowania, 4) fałszywym zaświadczeniem o prawie uczestnictwa w walnym zgromadzeniu spółki publicznej, 5) fałszywymi instrukcjami do głosowania na walnym zgromadzeniu spółki publicznej – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
Art. 592	Członek zarządu, który dopuszcza do wydania dokumentów akcji: 1) niedostatecznie opłaconych, 2) przed zarejestrowaniem spółki, 3) w przypadku podwyższenia kapitału zakładowego – przed zarejestrowaniem podwyższenia – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 594	§ 1. Kto, będąc członkiem zarządu spółki handlowej, wbrew obowiązkowi dopuszcza do tego, że zarząd: 1) nie składa sądowi rejestrowemu listy wspólników, 2) nie prowadzi księgi udziałów zgodnie z przepisami **art. 188** § 1 albo nie prowadzi księgi akcyjnej zgodnie z przepisami **art. 341** § 1, 3) nie zwołuje zgromadzenia wspólników albo walnego zgromadzenia, 4) odmawia wyjaśnień osobie powołanej do rewizji lub nie dopuszcza jej do pełnienia obowiązków, 5) nie przedstawia sądowi rejestrowemu wniosku o wyznaczenie biegłych rewidentów, 6) nie ogłasza wzmianki o złożeniu opinii przez biegłego rewidenta w sądzie rejestrowym zgodnie z przepisem **art. 312** § 7 – podlega grzywnie do 20 000 złotych. § 2. Kto, będąc członkiem zarządu, dopuszcza do tego, że spółka przez czas dłuższy niż trzy miesiące wbrew prawu lub umowie pozostaje bez rady nadzorczej w należytym składzie – podlega grzywnie w tej samej wysokości. § 3. Przepisy § 1 i § 2 stosuje się odpowiednio do likwidatorów. § 4. Grzywnę nakłada sąd rejestrowy.
Art. 595	§ 1. Kto, będąc członkiem zarządu spółki kapitałowej, dopuszcza do tego, że pisma i zamówienia handlowe oraz informacje, o których mowa w **art. 206** § 1 i **art. 374** § 1, nie zawierają danych określonych w tych przepisach albo będąc komplementariuszem spółki komandytowo-akcyjnej uprawnionym do reprezentowania spółki dopuszcza do tego, że pisma i zamówienia handlowe oraz informacje, o których mowa w **art. 127** § 5, nie zawierają danych określonych w tym przepisie – podlega grzywnie do 5000 złotych. § 2. Przepisy **art. 594** § 3 i § 4 stosuje się odpowiednio.

9.6. Pozakodeksowe typy czynów zabronionych na rynku finansowym

W polskim systemie normatywnym typy czynów zabronionych korelujące z zakresem przedmiotowym szeroko rozumianego rynku finansowego nie znajdują się wyłącznie w Kodeksie karnym, Kodeksie karnym skarbowym oraz Kodeksie spółek handlowych. W skład systemu prawnego w obszarze finansów wchodzi wiele ustaw szczegółowych, które regulują określone, częstokroć specjalistyczne wycinki tematyczne wymagające interwencji państwa. W ich skład wchodzą przepisy prawne należące do różnych gałęzi prawa w tym prawa cywilnego, administracyjnego i karnego. Czasami zdarza się, że przedmiotowe unormowania zawierają przepisy karne tworzące nowe typy czynów zabronionych, które nie znajdują się w kodeksach. Poniżej zaprezentowano przykłady wybranych typów czynów zabronionych znajdujących się w sferze pozakodeksowej.

Art. 156 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[393]	1. Kto, działając w imieniu lub na rzecz instytucji obowiązanej: 1) nie dopełnia obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, lub obowiązku przekazania Generalnemu Inspektorowi zawiadomienia o powzięciu uzasadnionego podejrzenia, że określona transakcja lub wartości majątkowe będące przedmiotem tej transakcji mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, 2) przekazuje Generalnemu Inspektorowi nieprawdziwe lub zataja prawdziwe dane dotyczące transakcji, rachunków lub osób, 3) podlega karze pozbawienia wolności od 3 miesięcy do lat 5. 2. Tej samej karze podlega, kto wbrew przepisom ustawy ujawnia osobom nieuprawnionym, posiadaczom rachunku lub osobom, których transakcja dotyczy, informacje zgromadzone zgodnie z ustawą lub wykorzystuje te informacje w sposób niezgodny z przepisami ustawy. 3. Jeżeli sprawca czynu określonego w ust. 1 pkt 1 lub ust. 2 działa nieumyślnie, podlega grzywnie.
Art. 370 ustawy z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji[394]	1. Kto będąc członkiem zarządu lub rady nadzorczej podmiotu objętego systemem gwarantowania, o którym mowa w art. 2 pkt 41 lit. a i b, doprowadza do powstania straty po stronie Funduszu w wyniku tego, że podmiot ten nie utworzył funduszu ochrony środków gwarantowanych albo nie utworzył go w odpowiedniej wysokości lub aktywa przeznaczone na fundusz ochrony środków gwarantowanych nie były lokowane w skarbowych papierach wartościowych lub bonach pieniężnych Narodowego Banku Polskiego lub deponowane w sposób, o którym mowa w art. 369 ust. 7 i 8, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. 2. Tej samej karze podlega członek zarządu lub rady nadzorczej podmiotu objętego systemem gwarantowania, o którym mowa w art. 2 pkt 41 lit. a i b, który doprowadza do powstania straty po stronie Funduszu, obciążając aktywa stanowiące.
Art. 20a ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym[395]	Kto utrudnia lub udaremnia przeprowadzenie czynności w postępowaniu wyjaśniającym, podlega grzywnie do 500 000 zł, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
Art. 24 ustawy z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami[396]	1. Kto bez wymaganego zezwolenia, o którym mowa w art. 16 ust. 1 lub 3, prowadzi system lub dokonuje zmian w zasadach jego funkcjonowania, nie wykonuje obowiązku zamknięcia systemu w oznaczonym terminie pomimo decyzji cofającej zezwolenie na jego prowadzenie lub decyzji nakazującej jego zamknięcie, podlega grzywnie do 5 000 000 zł. 2. Tej samej karze podlega, kto nie dopełnia obowiązku przekazania dokumentów, o którym mowa w art. 27 ust. 2. 3. Tej samej karze podlega, kto dopuszcza się czynu określonego w ust. 1 lub 2, działając w imieniu lub na rzecz osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

[393] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723, 1075, 1499, 2215; z 2019 r., poz. 125).

[394] Ustawa z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji (t.j. Dz.U. z 2017 r., poz. 1937, 2491; z 2018 r., poz. 685, 723, 1637, 2243; z 2019 r., poz. 326).

[395] Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. Dz.U. z 2019 r., poz. 298, 326).

[396] Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (t.j. Dz.U. z 2019 r., poz. 212).

Art. 522 ustawy z dnia 28 lutego 2003 r. Prawo upadłościowe[397]	1. Kto będąc dłużnikiem albo osobą uprawnioną do reprezentowania dłużnika, który jest osobą prawną lub spółką handlową niemającą osobowości prawnej, podaje we wniosku o ogłoszenie upadłości nieprawdziwe dane – podlega karze pozbawienia wolności od 3 miesięcy do lat 5. 2. Tej samej karze podlega, kto będąc dłużnikiem lub osobą uprawnioną do reprezentowania dłużnika, który jest osobą prawną lub spółką handlową niemającą osobowości prawnej, w postępowaniu w przedmiocie ogłoszenia upadłości podaje sądowi nieprawdziwe informacje co do stanu majątku dłużnika.
Art. 45 ustawy z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym[398]	Kto, działając w imieniu lub interesie podmiotu nadzorowanego, nie dopełnia obowiązku dokonania blokady rachunku, podlega grzywnie do 1 000 000 zł albo karze pozbawienia wolności do lat 3, albo obu tym karom łącznie.
Art. 46 ustawy z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym	1. Kto utrudnia lub udaremnia przeprowadzanie czynności w postępowaniu kontrolnym lub administracyjnym, podlega karze grzywny do 500 000 zł, karze ograniczenia wolności albo pozbawienia wolności do lat 2. 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w ust. 1, działając w imieniu lub w interesie osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawne
Art. 178 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi[399]	Kto bez wymaganego zezwolenia lub upoważnienia zawartego w odrębnych przepisach albo nie będąc do tego uprawnionym w inny sposób określony w ustawie, prowadzi działalność w zakresie obrotu instrumentami finansowymi, podlega grzywnie do 5 000 000 zł.
Art. 99 ustawy z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych[400]	1. Kto dokonuje oferty publicznej papierów wartościowych bez wymaganego ustawą: 1) zatwierdzenia prospektu emisyjnego lub jego udostępnienia do publicznej wiadomości albo 2) zatwierdzenia memorandum informacyjnego albo stwierdzenia równoważności informacji w memorandum informacyjnym z informacjami wymaganymi w prospekcie emisyjnym lub udostępnienia memorandum informacyjnego do publicznej wiadomości lub osobom, do których skierowana jest oferta publiczna, albo 3) dokumentu informacyjnego, o którym mowa w art. 38a, lub bez jego złożenia do Komisji lub udostępnienia do publicznej wiadomości lub osobom, do których skierowana jest oferta publiczna – podlega grzywnie do 10 000 000 zł albo karze pozbawienia wolności do lat 2, albo obu tym karom łącznie. 2. Tej samej karze podlega, kto na terytorium jednego państwa członkowskiego udostępnia 150 osobom lub większej liczbie osób lub nieoznaczonemu adresatowi, w dowolnej formie i w dowolny sposób, informacje w celu promowania bezpośrednio lub pośrednio nabycia lub objęcia papierów wartościowych lub zachęcania, bezpośrednio lub pośrednio, do nabycia lub objęcia tych papierów wartościowych, o ile udostępnianie to nie jest związane z ubieganiem się o dopuszczenie tych papierów wartościowych do obrotu na rynku regulowanym lub ofertą publiczną tych papierów wartościowych w rozumieniu art. 3 ust. 1. 3. Tej samej karze podlega, kto dopuszcza się czynu określonego w ust. 1 lub 2, działając w imieniu lub interesie osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej. 4. W przypadku mniejszej wagi sprawca czynu określonego w ust. 1–3 podlega grzywnie do 2 500 000 zł.

[397] Ustawa z dnia 28 lutego 2003 r. Prawo upadłościowe (t.j. Dz.U. 2019, poz. 498).

[398] Ustawa z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym (t.j. Dz.U. z 2018 r., poz. 1417, 2243).

[399] Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz.U. z 2018 r., poz. 2286, 2243, 2244).

[400] Ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (t.j. Dz.U. z 2018 r., poz. 512, 685).

Art. 37 ustawy z dnia 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych[401]	1. Kto dokonuje emisji listów zastawnych nie będąc do tego uprawniony lub przy emisji narusza obowiązki określone w art. 17–19 i 22–24, lub nie będąc uprawniony do emitowania listów zastawnych emitowane papiery wartościowe określa nazwą „list zastawny" lub inną nazwą, która zawiera te wyrazy, podlega grzywnie do 50 000 zł i karze pozbawienia wolności od 6 miesięcy do lat 5. 2. Tej samej karze podlega, kto dopuszcza się czynu, o którym mowa w ust. 1, działając w imieniu osoby prawnej. 3. Jeżeli sprawca nieumyślnie dopuszcza się czynu określonego w ust. 1 lub 2, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 2.
Art. 171 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe[402]	1. Kto bez zezwolenia prowadzi działalność polegającą na gromadzeniu środków pieniężnych innych osób fizycznych, osób prawnych lub jednostek organizacyjnych niemających osobowości prawnej, w celu udzielania kredytów, pożyczek pieniężnych lub obciążania ryzykiem tych środków w inny sposób, podlega grzywnie do 10 000 000 złotych i karze pozbawienia wolności do lat 5. 2. Tej samej karze podlega, kto, prowadząc działalność zarobkową wbrew warunkom określonym w ustawie, używa w nazwie jednostki organizacyjnej niebędącej bankiem lub do określenia jej działalności lub reklamy wyrazów „bank" lub „kasa". 3. Tej samej karze podlega także ten, kto dopuszcza się czynu określonego w ust. 1 lub 2 działając w imieniu lub w interesie osoby prawnej lub jednostki organizacyjnej niemającej osobowości prawnej. 4. Kto, będąc obowiązany do podania uprawnionym organom informacji dotyczących banku i klientów banku w zakresie ustalonym w ustawie, podaje nieprawdziwe lub zataja prawdziwe dane, podlega grzywnie i karze pozbawienia wolności do lat 3. 5. Kto, będąc obowiązany do zachowania tajemnicy bankowej, ujawnia lub wykorzystuje informacje stanowiące tajemnicę bankową, niezgodnie z upoważnieniem określonym w ustawie, podlega grzywnie do 1 000 000 złotych i karze pozbawienia wolności do lat 3. 6. Kto, będąc odpowiedzialnym za zapewnienie właściwego funkcjonowania wewnętrznej kontroli danych i informacji wymaganych w związku ze sprawowaniem nadzoru skonsolidowanego lub za udzielanie informacji i wyjaśnień na żądanie Komisji Nadzoru Finansowego, nie wykonuje ciążącego na nim obowiązku albo wykonuje go nierzetelnie lub nieterminowo, podlega grzywnie do 1 000 000 zł lub karze pozbawienia wolności do lat 3. 7. Kto, będąc odpowiedzialnym za sporządzenie lub przedstawienie Komisji Nadzoru Finansowego skonsolidowanego sprawozdania finansowego lub innych sprawozdań związanych z nadzorem skonsolidowanym, nie wykonuje ciążącego na nim obowiązku albo wykonuje go nierzetelnie lub nieterminowo, podlega grzywnie do 500 000 zł lub karze pozbawienia wolności do lat 2. 8. Kto, będąc do tego obowiązanym, nie przekazuje do instytucji utworzonej na podstawie art. 105 ust. 4 informacji o całkowitym wykonaniu zobowiązania albo jego wygaśnięciu, stwierdzeniu nieistnienia zobowiązania albo korekcie jego wysokości oraz o nowo powstałych zobowiązaniach w terminie 7 dni od wystąpienia zdarzenia uzasadniającego przekazanie informacji, podlega grzywnie do 30 000 złotych.

[401] Ustawa z dnia 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych (t.j. Dz.U. z 2016 r., poz. 1771; z 2018 r., poz. 2243).

[402] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz.U. z 2018 r., poz. 2187, 2243, 2354; z 2019 r., poz. 326).

Art. 77 ustawy z dnia 29 września 1994 r. o rachunkowości[403]	Kto wbrew przepisom ustawy dopuszcza do: 1) nieprowadzenia ksiąg rachunkowych, prowadzenia ich wbrew przepisom ustawy lub podawania w tych księgach nierzetelnych danych, 2) niesporządzenia sprawozdania finansowego, skonsolidowanego sprawozdania finansowego, sprawozdania z działalności, sprawozdania z działalności grupy kapitałowej, sprawozdania z płatności na rzecz administracji publicznej, skonsolidowanego sprawozdania z płatności na rzecz administracji publicznej, sporządzenia ich niezgodnie z przepisami ustawy lub zawarcia w tych sprawozdaniach nierzetelnych danych – podlega grzywnie lub karze pozbawienia wolności do lat 2, albo obu tym karom łącznie.
Art. 42 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej[404]	1. Kto, świadcząc usługi zaufania, wydaje certyfikat zawierający nieprawdziwe dane w celu popełnienia czynu zabronionego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. 2. Tej samej karze podlega, kto składa podpis elektroniczny lub pieczęć elektroniczną weryfikowane certyfikatem, o którym mowa w ust. 1, w celu popełnienia czynu zabronionego.

9.7. Katalog najważniejszych aktów prawnych na rynku finansowym

Katalog najważniejszych aktów prawnych w ramach analizowania rynku finansowego stanowi narzędzie pomocnicze dla dokonywania analiz związanych z rozwiązaniami prawnymi, w kontekście przeciwdziałania przyczynom przestępczości. Dzieje się tak dlatego, że wymierne rezultaty, wytyczne czy rekomendacje mogą przybrać postać postulatów *de lege ferenda* dla polskiego ustawodawcy. Zatem subsydiarny aspekt katalogu najważniejszych aktów prawnych dla rynku finansowego implikuje tezę o otwartym charakterze prezentowanego zbioru.

Dodatkowo warto zauważyć, że katalog aktów analizowanych w ramach prac projektowych nie ograniczał się wyłącznie do prawa karnego materialnego oraz procesowego, ale także obejmował swoim zasięgiem prawo cywilne oraz administracyjne, również w wymiarze materialnym oraz procesowym. Dzieje się tak dlatego, że zapobieganie przyczynom przestępczości na rynku finansowym nie jest tożsame przedmiotowo z zakresem prawa karnego, ale także innych regulacji, które mają znaczenie dla praktyki i teorii badanej płaszczyzny analitycznej.

Reasumując, w skład otwartego katalogu najważniejszych aktów prawnych składających się na szeroko rozumiany rynek finansowy można zaliczyć następujące źródła powszechnie obowiązującego prawa w Polsce:

[403] Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. Dz.U. z 2019 r., poz. 351).

[404] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2019 r., poz. 162).

- ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu;
- ustawa z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji;
- ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy;
- ustawa z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego[405];
- ustawa z dnia 15 kwietnia 2005 r. o nadzorze uzupełniającym nad instytucjami kredytowymi, zakładami ubezpieczeń i firmami inwestycyjnymi wchodzącymi w skład konglomeratu finansowego;
- ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych;
- ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych[406];
- ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego[407];
- ustawa z dnia 2 kwietnia 2004 r. o niektórych zabezpieczeniach finansowych[408];
- ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym;
- ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny[409];
- ustawa z dnia 23 listopad 2003 r. o świadczeniach rodzinnych[410];
- ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami;
- ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych[411];

---

[405] Ustawa z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego (t.j. Dz.U. z 2018 r., poz. 1530, 2161, 2193, 2245; z 2019 r., poz. 525).

[406] Ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (t.j. Dz.U. z 2018 r., poz. 1458, 1669 i 1693, 2192).

[407] Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (t.j. Dz.U. z 2018 r., poz. 1360, 1467, 1499, 1544, 1629, 1637, 1693, 2385, 2432; z 2019 r., poz. 55, 60).

[408] Ustawa z dnia 2 kwietnia 2004 r. o niektórych zabezpieczeniach finansowych (t.j. Dz.U. z 2016 r., poz. 891; z 2019 r., poz. 326).

[409] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2018 r., poz. 1025, 1104, 1629, 2073, 2244; z 2019 r., poz. 80).

[410] Ustawa z dnia 23 listopada 2003 r. o świadczeniach rodzinnych (t.j. Dz.U. z 2018 r., poz. 2220, 2354; z 2019 r., poz. 60. 303).

[411] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2017 r., poz. 2077; z 2018 r., poz. 62, 1000, 1366, 1669, 1693, 2245, 2354, 2500; z 2019 r., poz. 303, 326, 534).

- ustawa z dnia 28 lutego 2003 r. Prawo upadłościowe i naprawcze;
- ustawa z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym;
- ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi;
- ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych;
- ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa[412];
- ustawa z dnia 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych;
- ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim[413];
- ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe;
- ustawa z dnia 29 września 1994 r. o rachunkowości;
- ustawa z dnia 3 lutego 1993 r. o restrukturyzacji finansowej przedsiębiorstw i banków oraz o zmianie niektórych ustaw[414];
- ustawa z dnia 5 sierpnia 2015 r. o nadzorze makroostrożnościowym nad systemem finansowym i zarządzaniu kryzysowym w systemie finansowym[415];
- ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej;
- ustawa z dnia 6 czerwca 1997 r. – Kodeks karny;
- ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[416];
- ustawa z dnia 7 lipca 1994 r. o denominacji złotego[417].

---

[412] Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (t.j. Dz.U. z 2018 r., poz. 650, 723, 771, 800, 1000, 1039, 1075, 1499, 1540, 1544, 1629, 1693, 2126, 2193, 2244, 2354; z 2019 r. poz. 60).

[413] Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (t.j. Dz.U. z 2017 r., poz. 1373; z 2018 r. poz. 2243; z 2019 r., poz. 371).

[414] Ustawa z dnia 3 lutego 1993 r. o restrukturyzacji finansowej przedsiębiorstw i banków oraz o zmianie niektórych ustaw (opracowano na podstawie t.j. Dz.U. z 2018 r., poz. 1439).

[415] Ustawa z dnia 5 sierpnia 2015 r. o nadzorze makroostrożnościowym nad systemem finansowym i zarządzaniu kryzysowym w systemie finansowym (tj. z Dz.U. z 2019 r., poz. 483).

[416] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2018 r., poz. 1987, 2399; z 2019 r., poz. 150).

[417] Ustawa z dnia 7 lipca 1994 r. o denominacji złotego (Dz.U. z 1994 r. Nr 84, poz. 386; z 1995 r. Nr 16, poz. 79).

Sprawozdanie z warsztatu naukowego „Przeciwdziałanie przyczynom przestępczości na rynku finansowym" – 25 marca 2019 r.

W dniu 25 marca 2019 roku odbył się warsztat naukowy zorganizowany przez Instytut Wymiaru Sprawiedliwości. Wzięli w nim udział wybitni eksperci z zakresu rynku finansowego oraz osoby piastujące najważniejsze funkcje we własnych organizacjach.

Dr Marcin Wielec

Gości przywitał dr Marcin Wielec, zaznaczając, że warsztat naukowy to pierwsze wydarzenie z cyklu spotkań w ramach projektu „Prawo, gospodarka i technologia na rzecz zapobiegania przyczynom przestępczości".

Dr inż. Tomasz Kisielewicz

Gości przywitał również dr inż. Tomasz Kisielewicz, który wskazał, że jest mu niezmiernie miło, iż zgromadzeni uczestnicy wyrażają zainteresowanie projektem. Zaznaczył, że w ramach prac otrzymał wiele pozytywnych informacji zwrotnych, które mobilizują do kontynuacji podejmowanych działań.

Dr inż. Tomasz Kisielewicz wskazał także, że każda przekazana myśl zachęca do wypracowywania rezultatów zmierzających do zmniejszenia problemu przestępczości w sektorach finansowym, energetycznym, ubezpieczeniowym oraz zarządzania ludźmi w organizacji.

Bartłomiej Oręziak

Główne zagadnienia przestępczości na rynku finansowym wraz z głównymi założeniami Projektu przedstawił mgr Bartłomiej Oręziak. Podczas wystąpienia wskazał, że w ramach prowadzonych badań została pozyskana, a także

zaktualizowana, wiedza na temat zagranicznych rozwiązań w dziedzinie finansów oraz zagrożeń dla podstawowych zasad polskiego porządku prawnego.

Rekomendacje znajdują się w siedmiu segmentach analitycznych:

- Analiza rozwiązań organizacyjnych ułatwiających zachowanie kontroli instytucji finansowej nad operacjami realizowanymi przez jej pracowników w kontekście zapobiegania przyczynom przestępczości;
- Analiza procesu podejmowania decyzji w instytucjach finansowych w kontekście zapobiegania przyczynom przestępczości;
- Analiza zarządzania operacjami w instytucjach finansowych w kontekście zapobiegania przyczynom przestępczości;
- Analiza zarządzania ryzykiem w instytucjach finansowych w kontekście zapobiegania przyczynom przestępczości;
- Analiza przygotowania obrony przed różnymi formami ataków na instytucje finansowe w kontekście zapobiegania przyczynom przestępczości;
- Analiza działalności międzynarodowych grup przestępczych oraz metod zapobiegania im w instytucjach finansowych w kontekście zapobiegania przyczynom przestępczości;
- Analiza przestępstw finansowych dokonywanych przez klientów instytucji finansowych oraz metod zapobiegania im w kontekście zapobiegania przyczynom przestępczości.

Kierownik wykonawczy projektu dodał także, że prowadzone prace badawcze nie abstrahowały od problemów praw człowieka, gdzie dokonano analizy wpływu innowacyjności w konkretnych sytuacjach. Następnie zaprosił gości na panel Zespołu Implementacyjnego.

Dr Grzegorz Blicharz

Panel Zespołu Implementacyjnego „Przeciwdziałanie przestępczości na rynku finansowym: wyzwania współczesności" rozpoczął dr Grzegorz Blicharz, wskazując, że istnieje wiele poziomów przestępczości i sposobów jej przeciwdziałania, które opierają się na czynniku ludzkim. Okazuje się, że najwięcej bowiem zależy od postępowania zgodnie z dobrą wiarą (m.in. przez staranne dobieranie personelu i zwracanie uwagi na element etyczny), nie zaś tylko od regulacji prawnych.

Kultura organizacyjna jest stałą antropologiczną. Dokonano próby przeglądu wyzwań i regulacji oraz oceny zachęt i kar, które przyczynią się do ograniczenia przestępczości.

Grzegorz Blicharz wskazał, że celem Zespołu Implementacyjnego jest przedstawienie w siedmiu płaszczyznach analitycznych zarówno pewnych propozycji oraz rozwiązań dla prawodawcy, jak i sposobu regulacji.

Emil Ratowski

Podczas warsztatu wygłosił prelekcję pt. „Minimalizacja wystąpienia ryzyka oraz skutków oszustw wewnętrznych i zewnętrznych dotykających instytucji finansowych".

Emil Ratowski wskazał, że ryzyko oszustwa jest częścią ryzyka operacyjnego, gdzie nie można go wyeliminować z uwagi na motyw występowania, czyli chęć osiągnięcia zysku kosztem instytucji finansowej. Skomplikowana struktura organizacyjna firmy (organizacji) sprawia, że ryzyko związane z przestępczością jest większe.

Inna nazwa na oszustwo to pochodzące z angielskiego słowa *freud* – rozumiane zarówno jako „zamiar", jak i „zła wiara". Główną przyczyną przestępczości jest przekonanie o niemożliwości wykrycia skutków. Do przestępstwa dochodzi również w sytuacji, gdy więź między instytucją finansową a pracownikiem jest zbyt mała (np. poczucie odrzucenia przez instytucję finansową). Emil Ratowski wskazał główne motywy popełnienia przestępstwa:

- Okazję do popełnienia przestępstwa;
- Odczuwanie nacisku i presji (na przykład z powodu trudnej sytuacji finansowej pracownika);
- Zdolność do racjonalizowania swojego zachowania (tj. umiejętność pogodzenia wizji siebie jako osoby godnej zaufania razem z wizją osoby dokonującej przestępstwo).

Obszary, w których najczęściej dochodzi do przestępczości, to korupcja – łapówkarstwo, niekorzystne dla instytucji finansowej umowy, fałszowanie dokumentacji (najmniej) oraz sprzeniewierzenie środków finansowych instytucji (najwięcej).

Aby móc zarządzać ryzykiem, należy wskazać ramy, na podstawie których ustalimy plan działania dla konkretnej instytucji poprzez:

- Zdefiniowanie ryzyka operacyjnego na potrzeby określonej jednostki;

- Wybór metody pomiaru ryzyka oraz ograniczenia i kontroli;
- Wypracowanie procedur zapobiegania;
- Budżet, który powinien brać pod uwagę ziszczenie ryzyka (tak, aby jego pojawienie nie przerwało prac);
- Rozpoznanie ryzyka i jego pomiar – osoba z kwalifikacjami powinna identyfikować konkretne ryzyka i procedury.

Prelegent zauważył, że ryzyko można tolerować, jeśli zjawisko to rzadko występuje, a przy tym koszty są niewielkie. Przy średnim ryzyku i kosztach z nim związanych powinniśmy wprowadzić konkretne procedury w organizacji. Natomiast przy krytycznym ryzyku, które często występuje i niesie za sobą duże skutki, powinniśmy odstąpić od tej działalności.

Emil Ratowski wskazał również propozycje rozwiązań. Jedno z nich opiera się na ogromnej roli pracownika. Wiele zależy od standardów etycznych, które powinno się wypracować tak, aby pracownicy je znali i mogli informować o wszelkich nieprawidłowościach w instytucji. Kolejną propozycją zmiany jest bieżąca kontrola danych operacyjnych, bowiem aż 50% przyczynia się do redukcji strat związanych z oszustwem poprzez skrócenie czasu oszustwa. Następnym rozwiązaniem jest opracowanie reguł pracowniczych poprzez wskazanie tzw. gorącej linii, tj. platformy alarmującej, w której pracownicy oraz zarząd firmy na każdym etapie będą mogli się komunikować. Równie istotne są kompleksowe szkolenia dla pracowników. Metody przestępcze są coraz bardziej wyrafinowane, a pracownicy dzięki odbytym szkoleniom będą mogli lepiej je wykrywać i odpowiednio reagować. Szkolenia powinny zaszczepić pewne standardy, co przyczyni się do wykształcenia etycznego środowiska pracy w firmie. Zatem niezbędne jest:

- Przyjmowanie rozwiązań związanych z pracownikami;
- Bieżąca kontrola;
- Przeprowadzenie niezapowiedzianych audytów.

Podczas wystąpienia prelegent zaprezentował również propozycje rozwiązań dla konkretnych problemów:

- Okazja – poczucie, że przestępstwo można wykryć;
- Racjonalizacja – polityka firmy powinna również być ukierunkowana na zaszczepienie pewnych standardów etycznych, co przyczyni się do stworzenia etycznego środowiska;

- Nacisk, który powinien być eliminowany przez np. ubezpieczenia pracownicze, dzięki którym pracownik w przypadku pogorszenia stanu zdrowia nie jest pod naciskiem konieczności pozyskania funduszy.

Podsumowując, wskazał on, że nie da się całkowicie wyeliminować oszustw. Natomiast konieczna jest minimalizacja ryzyka, a kontrola procedur powinna być przeprowadzana cyklicznie. Powinno się również opracować pewne reguły. Najważniejsza jest jednak troska o pracownika i ukształtowanie go, tak aby nie godził się na nieprawidłowości, niezależnie od swojej pozycji i relacji z innymi pracownikami. Można tego dokonać poprzez przeprowadzenie szkoleń oraz wzbudzanie poczucia bezpieczeństwa w kontaktach z zarządem. Pracownicy nie mogą mieć przeczucia, że za dostarczenie informacji spotka ich kara. Wręcz przeciwnie, że może spotkać ich jakaś gratyfikacja.

Kamil Ratowski

Kamil Ratowski wygłosił prelekcję pt. „Przeciwdziałanie przestępstwom z wykorzystaniem walut wirtualnych".

Kamil Ratowski rozpoczął swoje wystąpienie od wskazania, iż pojęcie „walut wirtualnych" jest szersze niż pojęcie „kryptowalut". Wirtualne waluty są pojęciem trudnym do zdefiniowania i kontrowersyjnym. Przedstawiono również dwa podejścia do kryptowalut:

- Epokowy krok naprzód poprzez wyzwolenie płatności od polityki banków i narzędzie redukujące koszty, brak opłat transakcyjnych – szybciej niż konwencjonalnie;
- Stwarzają możliwość dla przestępców piorących pieniądze, finansujących terroryzm i unikających płacenia podatków – jest to swoista wada kryptowalut.

Występuje również wiele proponowanych definicji:

- Cyfrowe przedstawienie wartości – status prawny – nie ma mocy umarzania zobowiązań;
- Waluta wirtualna to nie jest cyfrowe odwzorowanie pieniądza;
- Środek wymiany i przedmiot transakcji – wirtualne odwzorowanie płatności.

Według V Dyrektywy AML waluta wirtualna to cyfrowe wyznaczniki wartości, które nie są emitowane ani gwarantowane przez bank centralny lub organ publiczny, nie muszą być powiązane z walutą prawnie obowiązującą

i nie posiadają prawnego statusu waluty lub pieniądza, lecz które są akceptowane przez osoby fizyczne lub prawne jako środek wymiany i mogą być przekazywane, przechowywane lub sprzedawane drogą elektroniczną.

Typy walut wirtualnych:

- Wymienialne – mogą być wymieniane na pieniądz (na przykład bitcoin);
- Niewymienialne – waluty te funkcjonują tylko w danym środowisku oraz nie mogą być wymieniane (na przykład w grach);
- Zcentralizowane – gdzie występuje 1 podmiot (tj. administrator), który kontroluje obieg;
- Zdecentralizowane – rozwiązania techniczne, ale nie występuje administrator (na przykład bitcoin).

Rozróżniamy następujące podmioty działające na rynku walut wirtualnych:

- *Excenger* – wymienia i pośredniczy w handlu;
- Administrator – zarządza;
- *User* (użytkownik) – dokonuje operacji finansowej, może nabywać na kilka sposobów;
- *Mainer* (górnik) – osoba, która poświęca swój sprzęt na rzecz systemu np. bitcoin weryfikacja transakcji, nagradza się go walutą;
- *Virtual currency wallet provider* – przechowuje walutę.

W swoim wystąpieniu Kamil Ratowski wskazał również, że w przypadku waluty wirtualnej istnieje ryzyko anonimowości indywidualnych podmiotów. Otóż użytkownik jest trudny do zidentyfikowania – może być zidentyfikowany tylko przez adres. Adres natomiast może być zmieniany przy próbie dokonania jednorazowej transakcji. Istnieją także podmioty, które zajmują się tworzeniem usług mających na celu utrudnianie identyfikacji podmiotu poprzez np. rozdrabnianie transakcji. Prelegent wskazał również na inne ryzyko, tj. na międzynarodowych charakter. Rozwiązania zastosowane w jednym kraju nie są uniwersalne, ponieważ można się zarejestrować w innym kraju, a działania powinny być realizowane z partnerami międzynarodowymi na poziomie Unii Europejskiej i wyższym.

Prelegent w swoim wystąpieniu przedstawił przykładowe przestępstwa z użyciem waluty wirtualnej:

- Ukrywanie źródeł pochodzenia dochodów;
- Finansowanie terroryzmu;
- Unikanie podatków.

Rozwiązania prawne w Polsce (mowa tutaj o Ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu) wyprzedziły nowatorskie rozwiązania zaproponowane przez Unię Europejską, gdzie została uregulowana kwestia m.in. nowych kategorii instytucji obowiązanych, np. użytkowników i kary do 1 mln zł lub 10 % obrotu oraz wprowadzono narzędzia dla instytucji kontroli.

Kamil Ratowski przedstawił również pewne rozwiązania organizacyjne i prawne:

- Powołanie podmiotu (jako wymóg obowiązkowy), który ponosiłby odpowiedzialność;
- Wymogi kapitałowe dla quasi-bankowych podmiotów – rzetelność przedsięwzięcia;
- Działanie globalne, bo krajowe jest niewystarczające;
- Waluty są kwestią kontrowersyjną i trzeba zadać sobie pytanie, czy wad nie będzie więcej niż zalet. Przez uregulowanie tej kwestii kryptowaluty mogą stracić swoją rację bytu;
- Zgoda społeczna – zaufanie jest podstawą dla funkcjonowania kryptowalut, a ich prawdziwość gwarantują użytkownicy.

Patryk Walczak

Patryk Walczak wygłosił prelekcję pt. „Systemy *compliance* a odpowiedzialność podmiotów zbiorowych".

Zaczynając swoje wystąpienie, Patryk Walczak wskazał przesłanki determinujące odpowiedzialność podmiotów zbiorowych. Następnie przedstawił uczestnikom relacje zachodzące pomiędzy *compliance* a odpowiedzialnością podmiotów zbiorowych.

Podczas wystąpienia Patryk Walczak przedstawił główne założenia projektu nowej ustawy:

- Koncepcję winy anonimowej, czyli poniesienie odpowiedzialności bez względu na fakt, czy znajdziemy winnego pracownika;
- Brak *compliance* – odpowiedzialność za brak systemu;
- Przeniesienie ciężaru dowodu. Jeżeli nie będzie systemu *compliance*, to właśnie na instytucji spocznie ciężar dowodu (a jeśli jest, to ciężar dowodu spocznie na prokuratorze);

- Pozycja procesowa podmiotu zbiorowego jest słabsza bez systemu *compliance*.

Zauważył on, że ciekawym do przytoczenia jest model, który występuje obecnie we Włoszech – model skrajnie administracyjny. Jeśli zostanie popełnione przestępstwo, to należy przypisać odpowiedzialność podmiotowi, chyba że przed przestępstwem wdrożono system *compliance*. W takiej sytuacji odpowiedzialność zostaje całkowicie wyłączona. Jeżeli podmiot wdroży system *compliance* przed procesem, ale już po przestępstwie, to można ograniczyć odpowiedzialność podmiotu zbiorowego.

Prelegent wskazał także, że system *compliance* oddziałuje również przez *occupation*, bowiem pracownik wykorzystuje swoją pozycję, aby uzyskać osobiste korzyści. Warto wskazać, że od końca lat 80. XX wieku obserwujemy zjawisko, w którym rola systemu *compliance* rośnie i jest użyteczna dla prawodawcy.

Patryk Walczak podczas swojego wystąpienia przedstawił także propozycje, zaadresowane do podmiotów zbiorowych:

- Powinno się wyodrębnić co najmniej jednego pracownika, który byłby odpowiedzialny tylko za badanie zgodności z pracownikami;
- Warto także uwolnić potencjał i zapewnić „kanał" pracownikom do anonimowego alarmowania zarządu o łamaniu standardów etycznych (tzw. wzmocnienie kontroli wewnętrznej).

Dr Grzegorz Blicharz

Dr Grzegorz Blicharz wskazał jak istotna jest ochrona sygnalistów. Przeważnie sygnalistą jest pracownik danej instytucji. Natomiast wątpliwe jest, czy jedna osoba jest w stanie przerwać spiralę przestępstw (ochrona przed odwetem ze strony instytucji).

Jeśli jesteśmy w posiadaniu wiedzy, że w organizacji istnieje kartel, należy to zgłosić (w tym miejscu został podniesiony apel, aby nie stosować odwetu oraz zapewnić anonimowość). Powinna być również możliwość zgłoszenia danego przypadku w formie telefonicznej, mailowej oraz elektronicznej (poprzez stworzenie specjalnego formularza).

Dr Grzegorz Blicharz przedstawił propozycję Dyrektywy Unii Europejskiej – model, który obecnie jest wykorzystywany w Wielkiej Brytanii. Model ten jest oparty na wewnętrznej informacji. Jeżeli następuje brak reakcji, to podmiot

powinien mieć możliwość kontaktu z podmiotami zewnętrznymi. Jeśli to rozwiązanie również nie przyniesie pozytywnych skutków, podmiot powinien przekazać informację mediom. Działanie to jednak nie może być obarczone negatywnymi konsekwencjami dla zgłaszającego podmiotu. Powinna być również zapewniona możliwość zewnętrznej ochrony sygnalistów np. przez przedstawiciela wymiaru sprawiedliwości, polski prawodawca zaproponował w projekcie prokuratora. Zatem od decyzji prokuratora przysługiwałoby odwołanie.

W swoim wystąpieniu prelegent omówił także rozwiązanie prawne, które jest stosowane w Ameryce. W ich regulacjach przoduje bowiem *whistleblower*. Sygnalista ma zapewnione środki ochronne oraz zagwarantowaną nagrodę za zgłoszenie przestępstwa, jeśli udało się mu przeciwdziałać. Wskazano również następujące sposoby ochrony:

- prawo Lincolna – aby dostawy dla armii nie były defraudowanie. Rozwiązanie polega na tym, że jeżeli zgłosiło się defraudację, to została wypłacona nagroda w wysokości 50% wartości tego, co udało się odzyskać, oraz 50% wartości pochodzących z nałożonych kar nałożonych (regulacja cywilnoprawna);
- regulacja skarbowa – możliwość wypłacenia nagrody osobie, która zgłosiła przestępstwo podatkowe o wartości przekraczającej 2 mln dolarów;
- regulacje wprowadzone w odpowiedzi na piramidę Madoffa i kryzys z 2008 r.

Prelegent wskazał więc następujące propozycje oraz rozwiązania organizacyjne:

- Program nagród dla sygnalistów oraz wskazanie poziomu nagród. Zgłoszenie nie jest łatwą ścieżką, ponieważ podmiot zgłaszający może się liczyć ze stratą pracy oraz potępieniem otoczenia. Jak wynika z danych, około 0,2% zgłoszeń jest nagradzana. Warto dodać, że sygnalistą nie musi być obywatel Ameryki;
- Według podanych informacji mały jest odsetek sygnalistów, którym zostały wypłacone nagrody. Powodem jest brak wystarczającej wiedzy na temat zachodzącego zjawiska. Pożądanym sygnalistą jest osoba posiadająca wiedzę o przestępstwie (a zatem jest pracownikiem lub byłym pracownikiem danej organizacji) oraz „mająca czyste ręce".

Nasuwa się pytanie, czy taka osoba posiada dostateczną wiedzę. Im mniej taka osoba przyczyniła się do popełniania przestępstwa, tym większa zostanie mu wypłacona nagroda. Warto wspomnieć, że udowodnienie strony podmiotowej wiąże się z przekazaniem informacji o swojej roli w popełnionym przestępstwie. Należy dodać, że aż 83% podmiotów zgłaszających przestępstwo przekazuje ten fakt najpierw w firmie (organizacji), a dopiero później informują o tym podmioty zewnętrzne.

- Im więcej zgłoszeń zewnętrznych, tym słabsze wydaje się *compliance* w danej organizacji, a to jest problematyczne, dlatego nie należy brać odwetu na sygnalistach. W zamian za to pracodawca powinien skierować większą uwagę na pracowników oraz o nich dbać.

Dr Grzegorz Blicharz zwrócił uwagę na pewne rozwiązania tego problemu, takie jak:

- Wewnętrzny i zewnętrzny system zgłoszeń o przestępstwie;
- Zapewniona nagroda finansowa dla osoby zgłaszającej lub zwolnienie jej z odpowiedzialności karnej.

Po wystąpieniu ostatniego eksperta Zespołu Implementacyjnego Rynku Finansowego zakończył się pierwszy panel warsztatu naukowego pt. „Przeciwdziałanie przyczynom przestępczości na rynku finansowym".

Po krótkiej przerwie rozpoczął się panel II zatytułowany „Grupa robocza". Polegał on na stworzeniu płaszczyzny wymiany poglądów, podczas którego uczestnicy wydarzenia mogli zabrać głos w dyskusji.

Panel dyskusyjny „Grupa Robocza"

Kierownik wykonawczy projektu otworzył panel dyskusyjny, zapraszając wszystkich zgromadzonych do zabrania głosu w dyskusji. Jego moderatorem został dr Grzegorz Blicharz. Uczestnicy podnieśli uwagę na następujące fakty:

- Należy zwracać większą uwagę na dywersyfikację ryzyka, na przykład rozdzielając działania. A zatem prowadzimy do powstania sytuacji, w której pracodawca nie tylko kontroluje pracowników, ale też rozdziela pomiędzy pracowników kompetencje;
- Należy unikać konfliktów interesów. Zdaniem uczestników konflikt interesów powodował brak powołania grupy sygnalistów. Kontrola

sama w sobie nie jest istotna, ale dywersyfikacja ryzyka i minimalizacja konfliktu interesów. Warto również zatrudnić dwóch specjalistów;

- Wskazano również na to, że etyka nie jest teraz ważna w organizacji (spycha się ją na margines). Należy ją przede wszystkim zaszczepiać w ludziach, bowiem często przekraczamy granice etyczne. Należy uczyć młodych ludzi, że etyka jest bardzo istotna;
- Najpierw trzeba stworzyć spójny system wartości dla organizacji (tj. dla zarządu oraz pracowników). Jeśli pojawi się dylemat, jak postąpić w danej sytuacji – można odwołać się do zadeklarowanego systemu wartości;
- Należy zacząć kontrolować tzw. czarny rynek (*dark web*). Jest opłacalny w kryptowalutach, a można je spieniężyć tylko na giełdach wymiany – dlatego to miejsce należy poddać wzmożonej kontroli;
- Ład korporacyjny – *compliance* trzeba wysoko osądzić, bo jeżeli dział *compliance* widzi nieetyczne działanie i będzie reagował nieskutecznie, to nie uda się zapobiec konsekwencjom.

Podczas II panelu uczestnicy próbowali odpowiedzieć także na pytanie, czy Polska jest gotowa na przyjęcie i wprowadzenie rozwiązań, które są stosowane w systemie amerykańskim. Zauważyli oni, że nagrody powinny być przyznawane w wewnętrznym trybie organizacji, nie zaś przez podmiot zewnętrzny. Praktyka wskazuje, że zgłoszenia zewnętrzne są przekazywane od osób pozostających w konflikcie z firmą. Natomiast fałszywe zawiadomienie powinno być penalizowane.

Podniesiono również kwestię, że działy *compliance* oraz HR powinny ze sobą współpracować, przede wszystkim w zakresie sporządzania regulaminów i opiniowania procedur.

Zdaniem jednego z uczestników powinno się przeprowadzać krótkie wywiady z osobami, które z różnych powodów rozwiązały stosunek pracy z daną organizacją. Często taka osoba nie ma oporów przed powiedzeniem prawdy oraz wskazaniem sytuacji panującej w firmie. Osoby te są źródłem merytorycznej wiedzy. Jednak należy pamiętać, aby zapewnić im zupełną anonimowość.

Po powyższym dr Marcin Wielec podziękował wszystkim zebranym zarówno za przybycie, jak i aktywny udział w dyskusji oraz zakończył warsztat naukowy dotyczący przeciwdziałania przyczynom przestępczości na rynku finansowym.

Bartłomiej Oręziak, Joanna Repeć, Dorota Sobczak

Bibliografia

Literatura

2018 Annual Report to Congress. Whistleblower Program, U.S. Securities and Exchange Commission 2018.

A Reformed Financial Sector for Europe. Commission Staff Working Document, European Commission, Brussels, 15 May 2014, COM(2014)279 final.

Agencja Bezpieczeństwa Wewnętrznego, *Metody prania pieniędzy*, http://www.abw.gov.pl/wolnytekst/69,dok.html [dostęp: 14.05.2019].

Ahlefeld H. von, Gaston J., *Lessons in Danger*, OECD Online Bookshop 2005.

Air Force Material Command Pamphlet. Acquisition: Risk Management, AFMC Pamphlet. 1997.

Al-Kaber M., *Struktura funkcjonalna rynku kapitałowego i jego sprawność w gospodarce współczesnej*, Białystok 2004.

Allard J., Blavy R., *Market Phoenixes and Banking Ducks. Are Recoveries Faster in Market-Based Economies?*, http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.893.4840&rep=rep1&type=pdf [dostęp:15.04.2019]

Ansell T., *Zarządzanie jakością w sektorze usług finansowych. Narzędzia zarządzania jakością oraz ich zastosowanie*, Warszawa 1997.

Bączyk M., *Umowy banku z jednostkami gospodarki uspołecznionej*, Toruń 1984.

Baer M.H., *Reconceptualizing the Whistleblower's Dilemma*, „UC Davis Law Review" 2017, no. 50.

Ballan E.J., *Protecting Whistleblowing (and Not Just Whistleblowers)*, „Michigan Law Review" 2017, no. 116, issue 3.

Bank und Börsenwesen, red. M. Bitz, München 1981.

Barlińska J., Małecka A., Świątkowska J., *Cyberbezpieczeństwo. Charakterystyka, mechanizmy i strategie zaradcze w makro i mikro skali*, Warszawa 2018.

Basel Committee on Banking Supervision, Operational Risk, Basel 2001.

Beck T., *Financial Development and Economic Growth. Stock Markets versus Banks?*, Tilburg 2010.

Bereza S., *Zarządzanie ryzykiem bankowym*, Warszawa 1992.

Bijlsma M.J., Zwart G.T.J., *The Changing Landscape of Financial Markets in Europe, the United States and Japan*, http://bruegel.org/wp-content/uploads/imported/publications/WP_2013_02_01.pdf [dostęp: 14.05.2019].

Bil J., Kulik M., Wojdak B., Bilewicz J., Jeżyński A., *Zorganizowana przestępczość transgraniczna*, Lublin 2015.

Binational Working Groupon Cross-Border Mass Marketing Fraud, Report on Phishing. A report to the Minister of Public Safety and Emergency PreparednessCanada and the Attorney General of the United States (2006).

Blicharz G., *Udział państwa w spadku. Rzymska myśl prawna w perspektywie prawnoporównawczej*, Kraków 2016.

Bolesta-Kukułka K., *Decyzje menedżerskie w teorii i praktyce zarządzania*, Warszawa 2003.

Boratyńska K.T., *Zwalczanie przestępczości w Unii Europejskiej. Współpraca sądowa i policyjna w sprawach karnych*, Warszawa 2006.

Bosua R., Milton S., Dreyfus S., Lederman R., *Going Public. Researching External Whistleblowing in a New Media Age*, [w:] *International Handbook on Whistleblowing Research*, red. A.J. Brown, D. Lewis, W. Vandekerckhove, Cheltenham–Northampton 2014.

Brière M., Oosterlinck K., Szafarz A., *Virtual Currency, Tangible Return. Portfolio Diversification with Bitcoin*, „Journal of Asset Management" 2015, no. 16(6).

Brown S., *Cryptocurrency and Criminality. The Bitcoin Opportunity*, „The Police Journal: Theory, Practice and Principles" 2016, no. 89(4).

Buczek S., *Efektywność informacyjna rynków akcji. Teoria a rzeczywistość*, Warszawa 2005.

Buszko A., *Finanse przestępczości zorganizowanej*, Toruń 2014.

Butler J.V., Serra D., Spagnolo G., *Motivating Whistleblowers*, Departmental Working Papers (2017) 1701, Southern Methodist University, Department of Economics.

Capiga M., *Reengineering kredytów detalicznych w polskiej praktyce bankowej*, „Bank i Kredyt" 2001, nr 8.

Capiga M., Harasim J., Szustak G., *Finanse banków*, Warszawa 2005.

Capiga M., *Zarządzanie bankiem*, Warszawa 2010.

Capiga M., *Ocena bezpieczeństwa funkcjonowania instytucji finansowych*, Warszawa 2013.

Capiga M., Szustak G., *Zarządzanie instytucjami finansowymi w niestabilnym otoczeniu gospodarczym*, Katowice 2014.

Capiga M., *Bezpieczeństwo transakcji finansowych w Polsce*, Warszawa 2015.

Chartis Research, *Financial Crime Risk Management Systems Oracle Vendor Highlights 2014*, http://www.oracle.com/us/corporate/analystreports/chartis-financial-crime-risk-2541655.pdf [dostęp: 13.05.2019].

Chodnicka P., *Pranie pieniędzy. Regulacje i ryzyko sektora bankowego*, Warszawa 2015.

Cichy Ł., *Funkcja compliance w bankach*, Warszawa 2015.

Ciszewska N., *Przestępstwa gospodarcze – istota i rodzaje*, „Studia nad Bezpieczeństwem" 2016, nr 1.
Clarke R.V., Cornish D.B., *Modelling Offenders Decisions. A Framework for Research and Policy*, „Crime and Justice" 1985, vol. 6.
Cohen L.E., Felson M., *Social Change and Crime Rate Trends*, „American Sociological Review" 1979, vol. 44.
Comparative Legal Guides, *Cybersecurity 2018*. https://acceurope2018.com/resources/20/The-International-Comparative-Legal-Guide-to-Cybersecurity-2018-1st-Edition.pdf [dostęp:13.05.2019].
Council of Europe – Convention on Cybercrime, ETS No. 185.
Culp C.L., *The Risk Management Process*, New Jersey 2001.
Czekaj J., *Rynki, instrumenty i instytucje finansowe*, Warszawa 2019.
Czekaj J., Woś M., Żarnowski J., *Efektywność giełdowego rynku akcji w Polsce. Z perspektywy dziesięciolecia*, Warszawa 2001.
Dahlgaard J.J., Kristensen K., Kanji G.K., *Podstawy zarządzania jakością*, Warszawa 2000.
Damasiewicz A., *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2010.
Decker R.J., *Homeland Security. Key Elements of a Risk Management Approach*, United States 2001.
Dibrova A., *Virtual Currency. New Step in Monetary Development*, „Procedia – Social and Behavioral Sciences" 2016, no. 229.
Dobosiewicz Z., *Bankowość*, Warszawa 2003.
Dobosiewicz Z., *Giełda. Zasady działania, inwestorzy, rynki giełdowe*, Warszawa 2013.
Drucker P.F., *What Makes an Effective Executive*, „Harvard Business Review" 2004, no. 6.
Dubs D., Truffer R., *Basler Kommentar*, Basel 2018.
Duży J., *Korzyści w przestępstwie prania pieniędzy*, „Prokuratura i Prawo" 2010, nr 12.
Duży J., *Zorganizowana przestępczość podatkowa w Polsce. Zwalczanie przestępczego nadużycia mechanizmów podatkowych VAT i akcyzowego*, Warszawa 2013.
Dziadek K., *Kontrola jako narzędzie wykrywania nieprawidłowości w wykorzystaniu funduszy unijnych*, „Zaszyty Naukowe Uniwersytetu Szczecińskiego" 2011, nr 669.
Epstein A., *The NCAA and Whistleblowers. 30–40 Years of Wrongdoing and College Sport and Possible Solutions*, „Southern Law Journal" 2018, no. 28.
Estimating the Economic Benefits of Whistleblower Protection in Public Procurement. Final report, „Przegląd Antykorupcyjny" 2016, nr 2(7).
European Banking Authority, *EBA Opinion on „virtual currencies"*, Londyn 2014. Europejski Bank Centralny, *Virtual Currency Schemes*, Frankfurt nad Menem 2012.
Fennelly L.J., *Handbook of Loss Prevention and Crime Prevention*, Amsterdam 2003.
Filar M., *Odpowiedzialność podmiotów zbiorowych za czyny zabronione pod groźbą kary*, [w:] *System prawa karnego*, t. 1, red. A. Marek, Warszawa 2010.

Financial Action Task Force – Groupe d'action financiere, Trade Based Money Laundering, Paryż 2006.

Financial Reform. A Framework for Financial Stability, Group of Thirty, 15 January 2009, http://fic.wharton.upenn.edu/fic/Policy%20page/G30Report.pdf [dostęp: 7.05.2019].

Fischer R.J., Green G., *Introduction to Security (7th Edn)*, Amsterdam 2004.

Fisiak J., *Słownik współczesny angielsko-polski, polsko-angielski*, Scarborough 2006.

Gawłowicz P., Wasilewicz M.A., *Międzynarodowa współpraca w walce z przestępczością*, Szczecin 2004.

Gill M., *Chapter 1. Introduction*, [w:] *Crime at Work Volume II. Increasing the Risk to Offenders*, red. *idem*, Leicester 1998.

Głowacka D., Ploszka A., Sczaniecki M., *„Wiem i powiem – ochrona sygnalistów i dziennikarskich źródeł informacji. Praktyczny przewodnik"* http://www.hfhr.pl/wp-content/uploads/2016/04/Wiem_i_powiem.pdf [dostęp: 16.05.2019].

Gołębiowska A., *Kradzież tożsamości w internecie*, Szczytno 2017.

Górecki M., *Informacje poufne na rynku kapitałowym – podstawowe problemy regulacji prawnej oraz pojęcie informacji poufnej i insidera*, „HUK" 2007, nr 1.

Górecki M., *Informacje poufne na rynku kapitałowym – obowiązki, procedury, sankcje*, „HUK" 2008, nr 1.

Górski M., *Rynkowy system finansowy*, Warszawa 2018.

GPW, *Dobre Praktyki Spółek Notowanych na GPW*, załącznik do Uchwały nr 12/1170/2007 Rady Giełdy z dnia 4 lipca 2007.

Grabosky P.N., Smith R.G., *Crime in the Digital Age. Controlling Telecommunications and Cyberspace Illegalities*, „Transaction Publishers" 1998, no. 1.

Grant I., *Wave of Criticism hits Government ID Card Relaunch in ComputerWeekly.com*, http://www.computerweekly.com/Articles/2008/03/07/229773/wave-of-criticism-hits-government-id-card-relaunch.htm [dostęp: 23.05.2019].

Gronkiewicz-Waltz H., Wierzbowski M., *Prawo gospodarcze*, Warszawa 2017.

Grzegorczyk W., *Rynek papierów wartościowych*, Łódź 1995.

Grzeszczak A., *Unia Europejska wobec przestępczości. Współpraca w ramach III filara*, Kraków 2002.

Grzywacz J., *Podstawy bankowości. System bankowy, kredyty i rozliczenia, ryzyko i ocena banku, marketing*, Warszawa 2006.

Grzywacz J., *Pranie pieniędzy: metody, raje podatkowe, zwalczanie*, Warszawa 2010.

Gurgul H., *Analiza zdarzeń na rynkach akcji. Wpływ informacji na ceny papierów wartościowych*, Kraków 2006.

Habrat D., *Ustawa o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary. Komentarz, Komentarz do art. 5*, Warszawa 2014.

Hatch M.J., *Teoria organizacji*, Warszawa 2002.

Heffernan S., *Nowoczesna bankowość*, Warszawa 2007.

Hertel F., *Qui Tam For Tax? Lessons From the States*, „Columbia Law Review" 2013, no. 113.

High-level Expert Group on Reforming the Structure of the EU Banking Sector, Chaired by Erkki Liikanen, Final Report, Brussels, 2 October 2012.
Hoare J., *Deceptive Evidence. Challenges in Measuring Fraud*, [w:] *Surveying Crime in the 21st Century*, red. J.M. Hough, and M.G. Maxfield, Cullompton 2007.
Hoffman T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.
Hofman K., *Banki zagraniczne w Europie środkowej. Wnioski z dotychczasowych doświadczeń*, Warszawa 2005.
Hołyst B., *Kryminalistyka*, Warszawa 2000.
Hołyst B., Pomykała J., *Cyberprzestępczość i ochrona informacji*, Warszawa 2012.
Horan D.J. *The Retailer's Guide to Loss Prevention and Security*, Floryda 1996.
Huffer U., Schaffer C., *Münchener Kommenta*, München 2010.
Independent Commission on Banking. *Final Report. Recommendations*, September 2011, http://www.ecgi.org/documents/icb_final_report_12sep2011.pdf [dostęp: 7.05.2019].
Iwanicz-Drozdowska M., *Zarządzanie finansowe bankiem*, Warszawa 2005.
Iwasaki M., *Effects of External Whistleblower Rewards on Internal Reporting*, „Harvard John M. Olin Fellow's Discussion Paper Series" 2018, no. 76.
Jadach K., *Wymiar sprawiedliwości w kontekście zakładanych funkcji kary*, „Studia Edukacyjne" 2013, nr 23.
Jagodziński B., *Rola wywiadu finansowego w przeciwdziałaniu procederowi prania pieniędzy i w jego zwalczaniu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7.
Jajuga K., *Zarządzanie ryzykiem*, Warszawa 2018.
Jakóbczak J., *Współczesne tendencje w zarządzaniu ryzykiem operacyjnym*, „Nasz Rynek Kapitałowy" 2003, nr 5.
Jara Z., *Kodeks spółek handlowych. Komentarz*, Warszawa 2017.
Jaroch W., *Zagrożenia systemu bankowego jako kategoria przestępczości gospodarczej. Zagrożenia w sektorze bankowym. Analiza kryminalna zjawisk oraz możliwości przeciwdziałania*, Olsztyn 2013.
Juja T., *Wydajność fiskalna podatku od towarów i usług w latach 2001–2007*, [w:] *Współczesne finanse. Stan i perspektywy rozwoju finansów publicznych*, red. J. Głuchowski, Toruń 2008.
Jurkowska-Zeidler Z., *Bezpieczeństwo rynku finansowego w świetle prawa Unii Europejskiej*, Warszawa 2008.
Kaczmarek T.T., *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2008.
Kapitalmarktstrafrecht, red. T. Park, Göttingen 2008.
Kaźmierczak P., *Instrumenty i realizacja polityki pieniężnej*, [w:] *Bankowość. Podręcznik akademicki*, Warszawa 2001.
Kendall R., *Zarządzanie ryzykiem dla menedżerów. Praktyczne podejście do kontrolowania ryzyka*, Warszawa 2000.
Kidyba A., *Kodeks spółek handlowych. Komentarz*, t. II, Warszawa 2017.

Klincewicz K., *Zarządzanie, organizacje i organizowanie – przegląd perspektyw teoretycznych*, Warszawa 2016.

Kobylińska A., Folta M., *Sygnaliści – ludzie, którzy nie potrafią milczeć. Doświadczenia osób ujawniających nieprawidłowości w instytucjach i firmach w Polsce*, Warszawa 2015.

Kokot-Stępień P., *Identyfikacja ryzyka jako kluczowy element zarządzania ryzykiem w przedsiębiorstwie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2015, nr 74, t. 1.

Kołecki H., Jęcz R., *Rola i zadania Narodowego Banku Polskiego oraz systemu bankowego w procesie zwalczania procederu prania pieniędzy w Polsce. Podstawowe uwarunkowania i kierunki działań*, [w:] *Proceder prania brudnych pieniędzy. Studia i materiały*, red. E. Pływaczewski, Toruń 1993.

Koleśnik J., *Bezpieczeństwo systemu bankowego. Teoria i praktyka*, Warszawa 2011.

Komisja Nadzoru Bankowego, *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*, Warszawa 2004.

Kordela D., *NewConnect – rynek giełdowy dla małych i średnich przedsiębiorstw. Systematyka, organizacja, perspektywy rozwoju*, Warszawa 2013.

Korenik D., *Innowacyjne usługi banku*, Warszawa 2006.

Kovacich G.L., Boni W.C., *High Technology Crime Investigator's Handbook*, Boston 2000.

Koźmiński A.K., Piotrowski W., *Zarządzanie. Teoria i praktyka*, Warszawa 1996.

Krasodomska J., *Zarządzanie ryzykiem operacyjnym w bankach*, Warszawa 2008.

Krawczyk A., Gisman A., *Criminal compliance jako środek zapobiegania odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary*, „Monitor Prawa Handlowego" 2015, nr 5.

Kubát M., *Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value*, „Procedia Economics and Finance" 2015, no. 30.

Kuciński R., *Przestępstwa giełdowe*, Warszawa 2000.

Kudła J., *Instrumenty finansowe i ich zastosowania*, Warszawa 2009.

Kulawik J., *Deregulacja systemów bankowych w wybranych krajach*, „Bank i Kredyt" 2003, nr 4.

Kulpaka P., *Giełdy w gospodarce*, Warszawa 2007.

Kurzajewski M., *Usługi maklerskie*, Warszawa 2014.

Łabuz P., Malinowska I., Michalski M., Safjański T., *Przestępczość gospodarcza. Istota zjawiska. Zasady odpowiedzialności, mechanizmy przestępcze i metody działania sprawców*, Warszawa 2017.

Levine R., *Bank-based or Market-based Financial Systems. Which is Better?*, „Journal of Financial Intermediation" 2002, vol. 11.

Levine R., *Finance and Growth. Theory and Evidence*, Amsterdam 2005.

Lewkowicz A., *Sektor bankowy z perspektywy cyberprzestępczości. Zagrożenia w sektorze bankowym. Analiza kryminalna zjawisk oraz możliwości przeciwdziałania*, Olsztyn 2013.

Liserre A., *Lezioni di diritto privato*, Mediolan 2017.
Lizak R., *Pranie pieniędzy w prawie polskim na tle europejskim, międzynarodowym i amerykańskim*, Warszawa 2018.
Longchamps de Bérier F., *Finansowa analiza prawa a znaczenie prawa rzymskiego*, „Forum Prawnicze" 2013, nr 5(19).
Loyens K., Vandekerckhove W., *Whistleblowing from an International Perspective. A Comparative Analysis of Institutional Arrangements*, „Administrative Sciences" 2018, vol. 8, issue 30.
Maderak K., *Ewolucja metod kwantyfikacji ryzyka*, „Bank" 2010, nr 9.
Majer I., *Podejście standardowe w Nowej Umowie Kapitałowej a procykliczność działalności kredytowej*, „Master of Business Administration. Pismo Wyższej Szkoły Przedsiębiorczości i Zarządzania im. L. Koźmińskiego i Międzynarodowej Szkoły Zarządzania" 2007, nr 2.
Małecka-Ziembińska E., *Luka w podatku od towarów i usług oraz sposoby jej ograniczania*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace / Szkoła Główna Handlowa" 2017, nr 1.
Manganelli R.L., Klein M.M., *Reengineering. Metoda usprawnienia negocjacji*, Warszawa 1998.
Manuale di istituzioni di diritto privato, a cura di M. di Pirro, Neapol 2018.
Martysz C., *Prawne i ekonomiczne aspekty karalności insider tradingu*, Warszawa 2013.
Matkowski P., *Zarządzanie ryzykiem operacyjnym*, Kraków 2006.
Mazur A., Pyka B., Utracka M., *Przestępstwa określone w prawie bankowym. Analiza art. 171 ustawy prawo bankowe. Problemy wykładnicze regulacji w świetle realiów obrotu bankowego*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 37.
McLaughlin E., Muncie J., *The Sage Dictionary of Criminology*, London 2006.
Merton R.C., *Operation and Regulation in Financial Intermediation. A Functional Perspective*, Stockholm 1993.
Michaels D., *U.S. Fines Billions for Wall Street Fraud. Nearly Half the Time It Doesn't Collect*, „The Wall Street Journal", 20.05.2019, https://www.wsj.com/articles/some-securities-fraudsters-escape-paying-sec-fines-11558344601 [dostęp: 16.07.2019].
Mishkin S., Eakins S.G., *Financial Markets and Institutions*, Boston 2015.
Morse E.A., *Whistleblowers and Tax Enforcement. Using Inside Information to Close the Tax Gap*, „Akron Tax Journal" 2009, vol. 24.
Munro M., Ford J., Leishman C., Karley N.K., *Lending to Higher Risk Borrowers. Sub-prime Credit and Sustainable Home Ownership*, The Homestead 2005.
Nawrot W., *Emisja akcji w Polsce w nowej europejskiej perspektywie. Jednolity rynek papierów wartościowych w Unii Europejskiej*, Warszawa 2006.
Near J.P., Niceli M.P., *After the Wrongdoing. What Managers Should Know About Whistleblowing*, „Business Horizons" 2016, no. 59.

Niedużak M.S., *Badanie występowania transakcji z wykorzystaniem informacji poufnych na Giełdzie Papierów Wartościowych w Warszawie*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2013, nr 904.
Nikolaou K., *ECB. Liquidity (Risk) Concepts. Definitions and Interactions*, Working Paper Series no. 1008, February 2009.
Nowak Z., Czerwińska T., *Rynek kapitałowy – efektywność i ryzyko*, Warszawa 2016.
O'Sullivan R., *„Private Justice" and FCPA Enforcement. Should the SEC Whistleblower Program Include a Qui Tam Provision?*, „American Criminal Law Review" 2016, no. 53.
Ochman P., *Ochrona działalności bankowej w prawie karnym. Przepisy karne ustaw bankowych*, Warszawa 2011.
Opitek P., *Skimming. Aspekty kryminalistyczne, cyberprzestępczość w bankowości elektronicznej*, Warszawa 2017.
Oplustil K., Wiórek P.M., *Europejskie i polskie regulacje dotyczące informacji poufnych na rynku kapitałowym (cz. I)*, „Prawo Spółek" 2005, nr 2.
Ostrowska E., *Rynek kapitałowy; funkcjonowanie i metody oceny*, Warszawa 2007.
Penc J., *Decyzje w zarządzaniu*, Kraków 1995.
Peppard J., Rowland R., *Reengineering*, Warszawa 1997.
Pietrzak B., Polański Z., Woźniak B., *System finansowy w Polsce*, Warszawa 2008.
Pływaczewski E., *Pranie brudnych pieniędzy nowym wyzwaniem dla systemu ekonomiczno-finansowego w Polsce*, [w:] *Proceder prania brudnych pieniędzy. Studia i materiały*, red. E. Pływaczewski, Toruń 1993.
Pływaczewski E.W., *Przestępczość zorganizowana*, Warszawa 2011.
Polański J., *Programy nagradzania informatorów w prawie państw europejskich*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, t. 3, nr 9.
Polska komparatystyka prawa. Prawo obce w doktrynie prawa polskiego, red. A. Wudarski, Warszawa 2016.
Połeć R., Lemańczyk M., *Przeciwdziałanie przestępczości ubezpieczeniowej w aspekcie jej społecznej akceptacji*, „Studia Oeconomica Posnaniesia" 2015, nr 11.
Policy Framework for Effective and Efficient Financial Regulation, Paris 2010.
Raczkowski K., *Bezpieczeństwo ekonomiczne obrotu gospodarczego. Ekonomia. Prawo. Zarządzanie*, Warszawa 2014.
Raport Kaspersky Lab Polska 2012.
Raport Symantec, www.symatec.com [dostęp: 14.05.2019].
Raport w sprawie masowej inwigilacji, Komitet ds. Prawnych i Praw Człowieka Zgromadzenia Parlamentarnego Rady Europy PACE (2015).
Raport w sprawie poprawy ochrony sygnalistów, Komitet ds. Prawnych i Praw Człowieka Zgromadzenia Parlamentarnego Rady Europy PACE (2015).
Redziak Z., *Podstawy teorii podejmowania decyzji*, Warszawa 2013.
Report to the Nations on Occupational Fraud and Abuse 2018 Global Fraud Study, Association of Certified Fraud Examiners.
Ressel E., *Rynek walutowy i pieniężny. Wprowadzenie*, Kraków 2010.

Ronickher A., *Cybersecurity Whistleblower Protections. An Overview of the Protections and Rewards Available to Cybersecurity Whistleblowers under Federal and State Law*, Washington 2017.
Rose P.S., Marquis M.H., *Financial Institutions and Markets*, New York 2011.
Rotsch T., *Criminal Compliance*, „Zeitschrift für Internationale Strafrechtsdogmatik" 2010, no. 10.
Samborski A., *Rynki papierów wartościowych w krajach Unii Europejskiej*, Katowice 2004.
Savage, Whistleblowers for Change. The Social and Economic Costs and Benefits of Leaking and Whistleblowing (2018).
Sawicka J., Marcinkowska E., Stronczek A., *Ujawnienie przestępstw prania pieniędzy przez pracowników zawodów księgowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, nr 34.
Schneider F., Raczkowski K., *Sfera nieoficjalna w gospodarce*, „Infos" 2013, nr 158.
Sferrazza M., *Appunti di diritto commerciale*, 2011.
Sharpe W., *Asset Allocation. Management Style and Performance Measurement*, „Journal of Portfolio Management", Winter 1992.
Siemieniuk N., Kilon J., *Technologie informatyczne na rynku kapitałowym*, Białystok 2006.
Sikorski G., *Prawo bankowe. Komentarz*, Warszawa 2015.
Simon H.A., *A Behavioral Model of Rational Choice*, „The Quarterly Journal of Economics" 1955, vol. 69, no. 1.
Simon H.A., *Models of Man, Social and Rational*, Oxford 1957.
Siwicki M., *Cyberprzestępczość*, Warszawa 2013.
Skorupka J., *Pojęcie „brudnych pieniędzy" w prawie karnym*, „Prokuratura i Prawo" 2006, nr 11.
Skrzypek E., *Zarządzanie ryzykiem i zmianami w organizacji*, Lublin 2015.
Smolak M., *Formy zwalczania procederu prania brudnych pieniędzy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.
Smyczek S., *Modele zachowań konsumentów na rynku usług finansowych*, Katowice 2007.
Sobol M., *System finansowy a wzrost gospodarczy*, „Studia Ekonomiczne Prawne i Administracyjne" 2015, nr 2.
Solarz J.K., *Zarządzanie ryzykiem systemu finansowego*, Warszawa 2005.
Song F., Thakor A.V., *Financial System Architecture and the Co-evolution of Banks and Capital Markets*, „Economic Journal" 2010, vol. 120.
Srokosz W., *Instytucje parabankowe w Polsce*, Warszawa 2011.
Stefański R.A., *Kodeks karny. Komentarz*, Warszawa 2017.
Submission to the Financial System Inquiry, March 2014, Reserve Bank of Australia, http://www.rba.gov.au/publications/submissions/fin-sys-inquiry-201403/pdf/fin-sys-inquiry-201403.pdf [dostęp: 5.04.2019].
Supernat J., *Racjonalność i logika decyzji administracji*, Warszawa 2008.

Świderski J., *Zarządzanie bankiem przez wartość*, „Bank i Kredyt" 1999, nr 1–2.
Szczepankiewicz E.I., *Wykorzystanie punktowej metody oszacowania ryzyka operacyjnego w instytucjach finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, nr 298.
Szczepankiewicz E.I., Wójtowicz A., *Model rejestru ryzyka w jednostkach sektora finansów publicznych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 76.
Szyszko L., *Finanse przedsiębiorstwa*, Warszawa 2007.
Talarek J., *Przestępczość w Polsce na tle wybranych krajów*, „Prawo. Ubezpieczenia. Reasekuracja" 2004, nr 2.
Tarczyński W., Mojsiewicz M., *Zarządzanie ryzykiem. Podstawowe zagadnienia*, Warszawa 2001.
Taylor J., *Internal Whistleblowing in the Public Service. A Matter of Trust*, „Public Administration Review" 2018, vol. 78, issue 5.
The Financial Action Task Force Report, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, Paryż 2014.
The High-level Group of Financial Supervision in the EU, chaired by Jacques de Larosiere, Final Report, Brussels, 25 February 2009, http://ec.europa.eu/internal_market/finances/docs/de_larosiere_report_en.pdf [dostęp: 5.04.2019]
Thiel S., *Rynek kapitałowy i terminowy*, Warszawa 2010.
Tokarczyk R., *Komparatystyka prawnicza*, Warszawa 2008.
Töpfer A.H., *Marktrisiken*, [w:] *Praxis des Risikomanagements*, red. D. Dörner, P. Horváth, P. Kagermann, Stuttgart 2000.
Tuzimek R., Bańkowski M., *Giełda papierów wartościowych w Warszawie – szanse i zagrożenia dalszego rozwoju*, [w:] *Rynki kapitałowe*, red. W. Bień, Warszawa 2005.
Uliasz R., *Nieważność uchwały zgromadzenia spółki kapitałowe*, Warszawa 2018.
Vinciguerra M.C., *Whistleblower Protection Legislation and Corruption*, *European Research Centre for Anti-Corruption and State-Building, Hertie School of Governance, Working Paper No. 52*, Berlin 2018.
Walczak W., *Rola fazy planowania w zarządzaniu projektami*, „E-mentor" 2010, nr 1(33).
Waszak M., *Status osób ujawniających nieprawidłowości w miejscu pracy w Republice Słowackiej i jego ewolucja z perspektywy przepisów ustawy z dnia 16 października 2014 roku*, [w:] *Etyka biznesu – wokół kluczowych zagadnień*, red. R. Sroka, Warszawa 2018.
Wilk L., *Przestępczość gospodarcza – pojęcie, przyczyny, sprawcy*, „Edukacja Prawnicza 2012, nr 10.
Wiśniewski P., Boehlke J., *Cyberprzestępczość w gospodarce*, Toruń 2017.
Wójcik J.W., *Pranie pieniędzy. Studium prawno-kryminologiczne i kryminalistyczne*, Toruń 1997.
Wolfe S., Worth M., Dreyfus S., *Protecting Whistleblowers in the UK. A New Blueprint*, London 2016.

Wróbel W., Zoll A., *Polskie prawo karne. Część ogólna*, Kraków 2014.
Zalewski W., *Lichwa*, [w:] *System prawa karnego*, red. R. Zawłocki, Warszawa 2015.
Zarządzanie firmą. Strategie, struktury, decyzje, tożsamość, oprac. Strategor [pseud. zbiorowy], Warszawa 1999.
Zawiła-Niedźwiecki J., *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji*, Kraków 2013.
Ziarko-Siwek U., *Ocena efektywności informacyjnej wybranych segmentów rynku finansowego w Polsce*, Warszawa 2004.
Zinkiewicz T., *Działalność inwestycyjna banków w świetle jednolitej licencji bankowej*, „Monitor Prawa Bankowego" 2016, nr 3.
Zoellick B., Frank T., *Governance, Risk Management, and Compliance. An Operational Approach. A Compliance Consortium Whitepaper*, https://gilbane.com/publications/GRC_Operational_Approach_PD1_0_050512.pdf [dostęp:16.05.2019].
Zoll F., *Prawo Bankowe*, t. 2: *Polsko-Niemieckie Centrum Prawa Bankowego UJ*, Kraków 2005.
Zoll F., *Prawo bankowe. Komentarz*, Kraków 2005.

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483; z 2001 r. Nr 28, poz. 319; z 2006 r. Nr 200, poz. 1471; z 2009 r. Nr 114, poz. 946).
Karta Praw Podstawowych Unii Europejskiej (Dziennik Urzędowy Unii Europejskiej C 326, 26.10.2012.
Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności (Dz.U. 1993 Nr 61, poz. 284).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (EU) nr 648/2012 (Dz.Urz. UE L 173 z 12.06.2014 r.).
Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (t.j. Dz.U. z 2018 r., poz. 1958, 2192, 2193, 2227, 2354).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2018 r., poz. 1600 z późn. zm.).
Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (t.j. Dz.U. 2019 poz. 505).
Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2018 r., poz. 723, 1075, 1499, 2215; z 2019 r., poz. 125).

Ustawa z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji (t.j. Dz.U. z 2017 r., poz. 1937, 2491; z 2018 r., poz. 685, 723, 1637, 2243; z 2019 r., poz. 326).
Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. Dz.U. z 2019 r., poz. 298, 326).
Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (t.j. Dz.U. z 2019 r., poz. 212).
Ustawa z dnia 28 lutego 2003 r. Prawo upadłościowe (t.j. Dz.U. 2019, poz. 498).
Ustawa z dnia 1 marca 2018 r. o zmianie ustawy o obrocie instrumentami finansowymi oraz niektórych innych ustaw (Dz.U. poz. 685).
Ustawa z dnia 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, (Dz.U. z 2018 r., poz. 723).
Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, (Dz.U. 1997 Nr 140, poz. 939 t.j.).
Ustawa z dnia 29 lipca 2005 r. o nadzorze nad rynkiem kapitałowym (t.j. Dz.U. z 2018 r., poz. 1417, 2243).
Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz.U. z 2018 r., poz. 2286, 2243, 2244).
Ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (t.j. Dz.U. z 2018 r., poz. 512, 685).
Ustawa z dnia 29 sierpnia 1997 r. o listach zastawnych i bankach hipotecznych (t.j. Dz.U. z 2016 r., poz. 1771; z 2018 r., poz. 2243).
Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz.U. z 2018 r., poz. 2187, 2243, 2354; z 2019 r., poz. 326).
Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. Dz.U. z 2019 r., poz. 351).
Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2019 r., poz. 162).
Ustawa z dnia 13 listopada 2003 r. o dochodach jednostek samorządu terytorialnego (t.j. Dz.U. z 2018 r., poz. 1530, 2161, 2193, 2245; z 2019 r., poz. 525).
Ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (t.j. Dz.U. z 2018 r., poz. 1458, 1669 i 1693, 2192).
Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (t.j. Dz.U. z 2018 r., poz. 1360, 1467, 1499, 1544, 1629, 1637, 1693, 2385, 2432; z 2019 r. poz. 55, 60).
Ustawa z dnia 2 kwietnia 2004 r. o niektórych zabezpieczeniach finansowych (t.j. Dz.U. z 2016 r., poz. 891; z 2019 r. poz. 326).
Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2018 r., poz. 1025, 1104, 1629, 2073, 2244; z 2019 r., poz. 80).
Ustawa z dnia 23 listopad 2003 r. o świadczeniach rodzinnych (t.j. Dz.U. z 2018 r., poz. 2220, 2354; z 2019 r., poz. 60, 303).
Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2017 r., poz. 2077; z 2018 r., poz. 62, 1000, 1366, 1669, 1693, 2245, 2354, 2500; z 2019 r., poz. 303, 326, 534).

Ustawa z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (t.j. Dz.U. z 2018 r., poz. 800, 650, 723, 771, 1000, 1039, 1075, 1499, 1540, 1544, 1629, 1693, 2126, 2193, 2244, 2354; z 2019 r., poz. 60).
Ustawa z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (t.j. Dz.U. z 2017 r., poz. 1373; z 2018 r., poz. 2243; z 2019 r., poz. 371).
Ustawa z dnia 3 lutego 1993 r. o restrukturyzacji finansowej przedsiębiorstw i banków oraz o zmianie niektórych ustaw (Opracowano na podstawie t.j. Dz.U. z 2018 r., poz. 1439).
Ustawa z dnia 5 sierpnia 2015 r. o nadzorze makroostrożnościowym nad systemem finansowym i zarządzaniu kryzysowym w systemie finansowym (tj. z Dz.U. z 2019 r., poz. 483).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2018 r., poz. 1987, 2399; z 2019 r., poz. 150).
Ustawa z dnia 7 lipca 1994 r. o denominacji złotego (Dz.U. z 1994 r. Nr 84, poz. 386, z 1995 r. Nr 16, poz. 79).
Uchwała nr 12/1170/2007 Rady Nadzorczej Giełdy Papierów Wartościowych w Warszawie S.A. z dnia 4 lipca 2007 r. w sprawie uchwalenia Dobrych Praktyk Spółek Notowanych na GPW, www.corp-gov.gpw.pl [dostęp: 15.05.2019].

Netografia

http://expertgroepklokkenluiders.nl/wp/wp-content/uploads/20150425-Whistleblowing-In-The-Netherlands.pdf [dostęp: 7.12.2018].
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ti_report_/ti_report_en.pdf [dostęp: 7.12.2018].
http://www.oecd.org/finance/financial-markets/1939320.pdf [dostęp: 5.12.2018].
https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/guidance-for-whistleblowers/ [dostęp: 8.12.2018].
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711355/180525_Financial_Crime_Compliance_Policy_Statement_v1.3b.pdf [dostęp: 5.12.2018].
https://blogs.worldbank.org/allaboutfinance/files/allaboutfinance/institutional_structures.pdf [dostęp: 5.12.2018].
https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=OJ:C:2007:306:TOC [dostęp: 13.05.2019].
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32005L0060 [dostęp: 13.05.2019].
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:11992M/TXT [dostęp: 13.05.2019].
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:11997D/TXT [dostęp: 13.05.2019].

https://eur-lex.europa.eu/resource.html?uri=cellar:a4e61a49-46d2-11e8-be1d-01aa75ed71a1.0013.02/DOC_1&format=PDF [dostęp: 7.12.2018].
https://www.dnb.nl/binaries/412714_DX0_DNB_OS_11-06_tcm46-301644.pdf [dostęp: 5.12.2018].
https://www.americanbar.org/content/dam/aba/migrated/poladv/priorities/privilegewaiver/2003jan20_privwaiv_dojthomp.authcheckdam.pdf [dostęp: 5.12.2018].
https://www.bankofengland.co.uk/-/media/boe/files/ccbs/ccbs-prospectus-2018 [dostęp: 5.12.2018].
https://www.borgesinternationalgroup.com/wp-content/uploads/sites/4/2018/06/2017-10-04-Criminal-Compliance-Policy_BIG_EN.pdf [dostęp: 5.12.2018].
https://www.cbr.cam.ac.uk/fileadmin/user_upload/centre-for-business-research/downloads/working-papers/wp407.pdf [dostęp: 8.12.2018].
https://www.chapman.com/media/publication/744_Chapman_Regulation_of_Marketplace_Lending_2018.pdf [dostęp: 5.12.2018].
https://www.dzp.pl/mailpic/compliance/raport_compliance_online.pdf [dostęp: 5.12.2018]
https://www.friedfrank.com/sitefiles/publications/cdb6714353b1b712d3a5db85f508483e.pdf [dostęp: 5.12.2018].
https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/3%20Pol%C3%ADtica%20de%20Compliance%20Penal_ENG.pdf [dostęp: 5.12.2018].
https://www.iaca.int/images/Research/Research_paper_05_Ruggero_Scaturro_final.pdf [dostęp: 8.12.2018].
https://www.imf.org/external/pubs/ft/fsa/eng/pdf/ch05.pdf [dostęp 5.12.2018].
https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_M_8_01_2013_uchwala_8_33017.pdf [dostęp: 14.05.2019].
https://www.ksiegarnia.beck.pl/17775-kodeks-karny-komentarz-alicja-grzeskowiak [dostęp: 31.05.2019].
http://www.transparency.sk/wp-content/uploads/2016/02/Whistleblower-protection-is-only-on-paper_ENG.pdf [dostęp: 7.12.2018].
https://rf.gov.pl/pdf/RAPORT%20UFK-CZ%202-WERSJA%20OST-30-03-2016%20pop.pdf [dostęp: 8.12.2018].
https://www.bis.org/fsi/publ/insights8.pdf [dostęp: 5.12.2018].
https://www.bis.org/fsi/publ/insights9.pdf [dostęp: 5.12.2018]. https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2018_50_signed.pdf [dostęp: 5.12.2018].
https://www.obegef.pt/i2fc/2015/DOCS/Pais.pdf [dostęp: 5.12.2018].
http://pclab.pl [dostęp: 14.05.2019].
https://piu.org.pl/public/upload/ibrowser/WU/WU1_2015/WU%201-2015%2009%20pabian%20wajda.pdf [dostęp: 8.12.2018].
https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-compliance-risk-assessments.pdf [dostęp: 22.12.2018].

Informacje o autorach

GRZEGORZ BLICHARZ – doktor nauk prawnych, magister filozofii, adiunkt w Katedrze Prawa Rzymskiego Uniwersytetu Jagiellońskiego, laureat stypendium MNiSW dla wybitnych młodych naukowców 2018–2021, ukończył Program for Development of Soft Skills and Entrepreneurship w Alberta School of Business, dyrektor Fundacji „Utriusque Iuris", członek redakcji czasopism „Forum Prawnicze" i „Prawo w Działaniu".

BARTŁOMIEJ ORĘZIAK – doktorant w Katedrze Ochrony Praw Człowieka i Prawa Międzynarodowego Humanitarnego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Laureat Stypendium Ministra Nauki i Szkolnictwa Wyższego za wybitne osiągnięcia naukowe na rok akademicki 2017/2018. Główne zainteresowania badawcze: prawo karne, prawo międzynarodowe, ochrona praw człowieka oraz prawo nowych technologii.

EMIL RATOWSKI – absolwent Wydziału Prawa i Administracji Uniwersytetu Warszawskiego, zastępca sekretarza redakcji czasopisma naukowego „Forum Prawnicze", praktykant w Biurze Interwencyjnej Pomocy Prawnej Kancelarii Prezydenta Rzeczypospolitej Polskiej, praktykant w Prokuratorii Generalnej Rzeczypospolitej Polskiej, asystent – wykonawca w projekcie naukowym „Ochrona Porządku Publicznego – wybrane aspekty prawnoporównawcze" realizowanego w ramach grantu badawczego „Polityka Sprawiedliwości 2018".

KAMIL RATOWSKI – absolwent Wydziału Prawa i Administracji Uniwersytetu Warszawskiego, zastępca sekretarza redakcji czasopisma naukowego „Forum Prawnicze", praktykant w Biurze Interwencyjnej Pomocy Prawnej Kancelarii Prezydenta Rzeczypospolitej Polskiej, praktykant w Prokuratorii Generalnej Rzeczypospolitej Polskiej, asystent w projekcie naukowym „Ochrona Porządku Publicznego – wybrane aspekty prawnoporównawcze" realizowanego w ramach grantu badawczego „Polityka Sprawiedliwości 2018".

PATRYK WALCZAK – absolwent Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego, student Uniwersytetu Padewskiego oraz sekretarz redakcji czasopisma naukowego „Forum Prawnicze". Autor pracy magisterskiej na temat potrącenia w prawie rzymskim. Został wyróżniony stypendium Ministra Nauki i Szkolnictwa Wyższego za wybitne osiągnięcia naukowe oraz stypendium Fundacji Lotto „100 na 100 im. H. Konopackiej i I. Matuszewskiego". Interesuje się prawem prywatnym oraz komparatystyką prawniczą.

MARCIN WIELEC – adiunkt w Katedrze Postępowania Karnego WPiA UKSW, P.O. kierownika Katedry Postępowania Karnego. Specjalista z zakresu prawa karnego procesowego, prawa karnego, prawa karnego wykonawczego oraz prawa karnego skarbowego, prawa i postępowania dyscyplinarnego. Autor artykułów naukowych, książek prawniczych i ekspertyz. Dyrektor Instytutu Wymiaru Sprawiedliwości, adwokat.