Maciej Aleksander Kędzierski[1]

Debanking/derisking wobec międzynarodowego systemu AML/CFT[2] oraz szczególnych rozwiązań dla instytucji obowiązanych wynikających z art. 41 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (część 1)

Cum tardius statuis, nitidioribus putes
(Kiedy decydujesz wolniej, myślisz mądrzej)
M. A. Kędzierski

Streszczenie

Przedsięwzięcia określane jako debanking *i* derisking *nie powinny być mylone z racjonalnie wykonywanymi i prawnie ustalonymi procedurami przeciwdziałania praniu pieniędzy czy finansowania terroryzmu. Rodzajowe niedopuszczanie do produktów i usług instytucji obowiązanych nie ma racjonalnego uzasadnienia w zakresie zapewniania bezpieczeństwa finansowego czy gospodarczego. W konsekwencji te dwa rodzaje działań mogą przyczyniać się do wzrostu zagrożenia i odejścia potencjalnych klientów do obszaru czarnej i szarej sfery gospodarczej.*

Słowa kluczowe

Debanking, derisking*, AML/CFT, ryzyko, identyfikacja, mityganty, środki bezpieczeństwa finansowego.*

1. Uwagi wprowadzające

„*Debanking*" to wycofanie lub odmowa świadczenia usług bankowych lub finansowych z powodu rzeczywistego lub domniemanego ryzyka równowa-

[1] dr Maciej Aleksander Kędzierski, radca prawny, ORCID: https://orcid.org/0000-0003-3074-1355.
[2] Angielski skrótowiec oznaczający: Anti-Money Laundering/Counter Financing of Terrorism (przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu).

żonego względami komercyjnymi danej instytucji usługodawczej (tę sytuację, szerzej, poza instytucją bankową, określa się jako *derisking*). D. Salampasis z Swinburne University of Technology, *debanking* definiuje jako: odmowa usług bankowych, odnosi się do zachowań przyjętych przez bankowe i niebankowe instytucje finansowe, które mają możliwość odmowy świadczenia usług, ograniczenia lub nawet zamknięcia konta klienta i relacji z klientem, ogólnie (osoby fizycznej, firmy lub kraju), co skutkuje utratą dostępu do regulowanego światowego systemu finansowego[3]. Jest on traktowany jako niekonkurencyjna praktyka polegająca na tym, że banki o ugruntowanej pozycji zaprzestają współpracy z innowacyjnymi lub naznaczonym powszechnie podmiotami, często z fałszywych powodów. Nie jest to jednak działanie, które podlega penalizacji. *Debanking* jest pojęciem pojemnym i może dotyczyć zarówno krajów i gospodarek, jak i firm lub uczestników niektórych branż (rodzajów, kategorii) związanych z wysokim ryzykiem, ale także może dotyczyć pojedynczych osób fizycznych. Wydaje się, że *debanking* można określić jako jedną z odmian szerszego pojęcia – *deriskingu*. W dalszej części artykułu, przedmiotowe rozważania w zakresie *debanking-u/derisking-u* wobec zachowań instytucji obowiązanych będą prowadzone także na podstawie przepisów ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (zwanej dalej: ustawą o p.p.p.f.t.)[4]. *Debanking* nie jest związany wyłącznie z obszarem przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Tego rodzaju zachowania instytucji finansowych można odnieść także do podmiotów związanych z proliferacją broni, sankcjami ekonomicznymi, politycznym, gospodarczymi[5]. W tym ostatnim przypadku, kluczowym czynnikiem ograniczającym dostęp do usług finansowych jest poziom uzyskiwanych dochodów. Wykluczenie finansowe dotyczy ograniczeń w dostępie do usług finansowych, spośród których szczególną uwagę zwraca się na usługi bankowe[6].

[3] The Senate Select Committee on Australia as a Technology and Financial Centre, Final report, October 2021, s. 83, (w:) https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024747/toc_pdf/Finalreport.pdf;fileType=application%2Fpdf.

[4] Dz. U. z 2022 r., poz. 593, 655, 835, 2180, 2185; z 2023 r., poz. 180, 326.

[5] W 2016 r. odmówiono założenia konta dla obywatela Iranu, mimo że miał kartę pobytu czasowego na terenie Polski. Związek Banków Polskich uzasadnił: odmowa założenia rachunku bankowego wynika z konieczności respektowania szczególnych środków ograniczających (sankcji międzynarodowych) i zapisów ustawy z dnia 16 listopada 2000 r. o [przeciwdziałaniu] praniu pieniędzy oraz finansowaniu terroryzmu (przy. aut. aktualnie nie obowiązuje). Z opinii Narodowego Banku Polskiego czy Generalnego Inspektora IF wynikało jednak, że w przepisach prawa nie ma podstaw do odmowy założenia rachunku dla obywateli Iranu. Nawet przy uwzględnieniu wytycznych i rekomendacji uznających Islamską Republikę Iranu za kraj wysokiego ryzyka, (w:) A. Jędrzejczyk, Kłopoty cudzoziemca z kontem w polskim banku, (w:) https://bip.brpo.gov.pl/pl/content/kłopoty-cudzoziemca-z-kontem-w-polskim-banku.

[6] B. Czerwiński, Zjawisko wykluczenia na rynku usług finansowych, (w:) Wyzwania współczesnych rynków finansowych. Praca zbiorowa pod red. nauk. L. Gąsiorkiewicza,

W innych przypadkach wykluczenie wiąże się z obawami o własne ryzyko instytucji, prestiż i realny wzrost bezpośredniego zagrożenia dla świadczonych usług (przekroczenie apetytu na ryzyko). Niejednokrotnie można zauważyć, że szeroko rozprzestrzenione zjawiska (głównie negatywne) powodują zwielokrotnioną obawę i generalizację odrzucenia oraz niezajmowanie się pojedynczymi przypadkami. Podmiot, który może być dotknięty takimi zjawiskami, nie stać (koszty finansowe) i nie chce dociekać głębiej źródła i ocen przyglądając się poszczególnym sprawom (nie dopuszcza oceny ryzyka) a w konsekwencji całościowo odrzuca „zjawisko zagrożenia" (obawa o koszt społeczny i osobisty). Elementy *debankingu*, czyli polityki „równoważenia" ryzyka instytucjonalnego wobec określonego rodzaju klientów, a raczej polityki odrzucenia świadczenia usług bankowych wobec określonych kategorii klientów, można więc doszukać się w różnych rozwiązaniach prawnych i faktycznych. Ten rodzaj działania można będzie określić także w kategorii świadomego transferu ryzyka na inne podmioty i w inne obszary (np. niezwiązane z ponoszeniem kosztów i odpowiedzialności w systemie AML/CFT). To zbliża przedmiotowe pojęcie (w sensie dynamicznym) do sterowania zagrożeniem (ryzykiem instytucjonalnym) poprzez pozorowane odrzucanie strat własnych. Przyczyny *debanking-u* mogą obejmować:
– względy handlowe, na przykład opłacalność świadczenia usług bankowych klientom wysokiego ryzyka;
– ryzyko utraty dobrej reputacji;
– niepewność związaną z modelem biznesowym klientów, zwłaszcza przedsiębiorstw wschodzących;
– szersze względy instytucji w zakresie polityki środowiskowej, społecznej i korporacyjnej;
– oczekiwania zagranicznych banków korespondentów w stosunku do instytucji krajowych;
– zgodność z wymogami sankcji;
– zgodność z wymogami dotyczącymi przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu[7].

2. Merytoryczne podstawy zastosowania *deriskingu* i *debankingu*

Wydawałoby się, że uporządkowana i przemyślana, w swoich początkowych założeniach, polityka międzynarodowa w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu doprowadziła do nieoczekiwanych konsekwencji ubocznych w postaci *debankingu* i *deriskingu*. Zakres

J. M o n k i e w i c z a, Warszawa 2019, s. 77, (w:) file:///C:/Users/HP/Downloads/Wyzwania%20wspolczesnych%20rynkow%20finansowych%20(2).pdf.

[7] D. J a c o b s o n, DE-BANKING RISKS, (w:) https://www.brightlaw.com.au/de-banking-risks/.

tych przedsięwzięć wywodzi się zwłaszcza z przyjmowania w instytucjach obowiązanych tzw. ogólnych zasad ograniczania ryzyka. Tym samym w zakresie zarządzania w banku rodzajem ryzyka, polegającego na: identyfikacji, ocenie, zastosowaniu narzędzi redukcji ryzyka, monitorowaniu efektywności redukcji ryzyka, raportowaniu, dochodzi jeszcze jeden „czynnik" wypowiedzenie lub niezawarcie umów. Wobec tego rodzaju ryzyk przeciwdziałaniem było zwłaszcza wykonywanie obowiązków AML/CFT oraz zwiększanie funduszy rezerwowych, mających zabezpieczyć instytucje obowiązane przed stratami. Przy czym wypowiedzenie świadczenia produktów czy usług może być efektem lub niemożliwością zrealizowania określonych czynności i stanowić *lex specialis* wobec ogólnych zachowań lub może być elementem ogólnej, wewnętrznej przyjętej polityki bezpieczeństwa w instytucji obowiązanej. Niemniej jednak *debanking*, czy *derisking* nie powinny mieścić się w prawidłowym zarządzaniu ryzykiem, jeżeli nie mieści się ono w ocenie określonej w art. 41 ust 1 ustawy o p.p.p.f.t. To nie zarządzanie ryzykiem a wręcz techniczno-organizacyjne wyzbywanie się klienta będącego nośnikiem ryzyka. Podejmowane w tym zakresie „działania" nie neutralizują ryzyka tylko przenoszą je w inny obszar (transferują), czasami bardziej niebezpieczny dla globalnego bezpieczeństwa, w tym bezpieczeństwa finansowego (również pośrednio/zwrotnie dla tych instytucji). Tego typu postępowanie instytucji obowiązanych może dotyczyć: klientów mających powiązania z jurysdykcjami, które są związane z wyższym ryzykiem ML/TF (zwłaszcza dotyczy to „państwa trzeciego wysokiego ryzyka", określonych przez Komisję Europejską), organizacji *non-profit*, klientów, wobec których z założenia należy stosować wzmożone środki bezpieczeństwa finansowego (np. PEP[8], osób zajmujących eksponowane stanowiska polityczne), będących nieodłącznie nośnikami wyższego ryzyka ML/FT, klientów znajdujących się na innych listach sankcyjnych niż listy ONZ/UE. Ale także przedmiotowe radykalne działania mogą dotyczyć klientów-podmiotów, których aktywność łączy się z wysokim obrotem gotówkowym, prezentujących nietypowy model prowadzenia biznesu, pozostających w negatywnej ocenie instytucji obowiązanej – wobec niemożliwości ustalenia beneficjenta rzeczywistego. Przedstawione kategorie proweniencji ryzyk mogą przekraczać apetyt na ryzyko w ocenie danej instytucji, jako ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu bądź też hybrydową aktywnością w biznesie. Ponadto w ocenie instytucji tego typu ryzyka mogą także stwarzać ryzyko prawne, operacyjne i utraty reputacji co może mieć także dalsze konsekwencje w sektorze świadczonych przez nią usług[9]. Wydaje się, że wobec takich

[8] Ang. *Politically Exposed Persons*.

[9] Apetyt na ryzyko (ang*. risk apetite*) – szeroko rozumiana wielkość ryzyka, jakie organizacja jest gotowa podjąć (zaakceptować), w celu realizacji swojej misji (lub wizji), (w:) https://ryzyko.pro/baza-wiedzy/apetyt-na-ryzyko/.

konsekwencji instytucja obowiązana posiada, subiektywnie stwierdzone, obawy nieporadzenia sobie z ryzykiem a tym samym uznaje, że najlepszym dla niej (czyli również subiektywnie wykreowanym wynikiem) będzie całkowite odrzucenie nośnika tego ryzyka, zwłaszcza poprzez niepodejmowanie relacji. *Debanking* jest swoistym stanowiskiem defensywnym instytucji obowiązanej wobec możliwego, a może nawet zakładanego *a priori* stanowiska wobec nośników (potencjalnych klientów) stanu niepewności.

Ponadto należy zauważyć, że *debanking*, czy *derisking* jest działaniem samodzielnym instytucji w celu realizacji subiektywnie ocenionego potencjalnego lub rzeczywistego ryzyka dla niedopuszczenia do jego wystąpienia poprzez wejście w relacji z danym podmiotem lub dalszego utrzymywania dotychczasowych relacji. W pierwszym przypadku, jest to działanie samoistne, dopuszczalne jednak nie jest to działanie, które mieści się w granicy obowiązków jakie musi spełnić instytucja w systemie przeciwdziałania (np. dla systemu n–AML/CFT). Ten drugi przypadek związany z AML/CFT, jest realizowany jako obowiązek określonego zachowania w związku z zaistniałą sytuacją. Stanowi więc przedmiot regulacji i może być efektem niemożności określenia wielkości i rodzaju ryzyka, a tym samym też niemożności zastosowania czynników przeciwdziałających ryzyku. Wydaje się, że w tym zakresie negatywna ocena dotyczy zwłaszcza podmiotów indywidualnych wywodzących się z obszaru danego rodzaju (np. sektora przekazów pieniężnych). I może być związana z niemożnością oceny ryzyka lub zbyt wysoką oceną ryzyka (np. wobec apetytu na ryzyko) w danym czasie odnoszącą się zarówno do całości takiego sektora, jak i poszczególnych podmiotów wchodzących w jego skład. Możliwym jest jednak zmiana takiego stanowiska wobec dokonania „wyceny" i określenia prawdopodobieństwa ryzyka sektora danego rodzaju, i to niekoniecznie wykonana przez określoną instytucję obowiązaną (autorem oceny może być np. FATF[10], Bank Światowy czy Europejski Urząd Nadzoru Bankowego)[11]. W konsekwencji będzie można otrzymać ogólne warunki ryzyka, które w sposób indywidualny oraz w zależności od charakteru i wielkości instytucji obowiązanej powinny być przez nią indywidualnie implementowane w ramach przygotowania instytucjonalnej oceny ryzyka. Ogólna ocena może być więc także wynikiem zastosowania outsourcingu wobec merytorycznych decyzji jakie w zakresie identyfikacji i oceny ryzyka należy podjąć w instytucji obowiązanej. Taka zmiana stanu rzeczy może także wpływać na zmianę postawy instytucji i dopuszczania podmiotów pochodzących z danego rodzaju sektora do obsługi w ramach świadczonych produktów i usług. Decydent dla sytuacji n–AML/CFT w zakresie zastosowania *debankingu*, czy *deriskingu*, opiera się na generalnych ustale-

[10] The Financial Action Task Force.

[11] Ale także może być to wynik wniosków określonych w Sprawozdaniu Komisji Europejskiej, o którym mowa w art. 6 ust. 1–3 dyrektywy 2015/849.

niach, iż „coś" lub „ktoś" niesie za sobą ryzyko i nie dopuszcza tych czynników do swojego podmiotu. Dla niego taki stan jest stanem niepewności (stanem subiektywnie odczuwanym przez podmiot decyzyjny), nie zaś stanem prawdopodobieństwa wystąpienia ryzyka (obiektywnej oceny). W przypadku prawdopodobieństwa, wynik może być znany, wyliczalny z określonym prawdopodobieństwem natomiast w stanie niepewności decydent pozostaje bez znajomości rozkładów prawdopodobieństwa. W takiej sytuacji zwiększają się także obawy decydenta co do skutków mającej być podjętej decyzji. Kalkulacja subiektywna powoduje, iż najbezpieczniejszym dla niego wyjściem będzie po prostu zadecydowanie się na odrzucenie w całości stanów generujących zagrożenie. Budując tym samym zapory już na dalekim przedpolu działań rozpoznawczych opartych na analizie ryzyka instytucjonalnego i indywidualnego. Jest to więc postawa świadomego wyzbywania się zarządzania ryzykiem. Dotyczyć to może wykluczenia z obsługi podmiotów kojarzonych z rynkiem kryptowalut, czy z rejestracją podmiotu gospodarczego w strefach *off-shore*/rajach podatkowych. Nie godzi się tym samym więc – jako decydent – na identyfikację, ocenę i zarzadzanie ryzykiem podejmując działania wyprzedzające np. zakazując podpisywania umów o prowadzenie konta bankowego z giełdą kryptowalut, czy nienadzorowanymi pośrednikami wymiany finansowej. Tym samym nie godzi się na prowadzenie wewnątrzinstytucjonalnej obsługi określonych rodzajowo, terytorialnie, czy zdarzeniowo podmiotów. Z pewnością tego typu zachowania instytucji nie mogą stać się normą lub mieć zjawiskowy charakter. W przypadku uznania ich za takie powinny być one traktowane jako zachowania kryminogenne i wymagające uregulowania prawnego przeciwstawnego wobec wskazanych postaw. Alternatywą wobec wskazanych powyżej radykalnych działań jest rozumienie ryzyka i doskonalenie oraz ustalanie nowych metod przeciwdziałania jemu.

Derisking może być także realizowany jako nieuzasadnione powoływanie się na art. 14 ust. 4 dyrektywy (UE) 2015/849[12], wobec całych kategorii (rodzajów) klientów bez należytego ich indywidualnego profilowania. Takie podejście może skutkować wykluczeniem finansowym całych grup klientów. W konsekwencji racjonalna regulacja może okazać się w swoim wykonawstwie zjawiskiem patologicznym. Efektem może być budowanie alternatywnych sposobów finansowania i przepływu środków, czyli mechanizmów niewidocznych dla organów odpowiedzialnych za bezpieczeństwo finansowe. Nienawiązywanie lub zerwanie relacji biznesowej lub nieprzeprowadzanie

[12] Dyrektywa 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, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Tekst mający znaczenie dla EOG), (w:) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32015L0849.

transakcji pozostaje w zgodności z przepisami dyrektywy 2015/849 z dnia 20 maja 2015 r., jednakże wektorowo powinno być ono stosowane wobec profili indywidualnych klientów nie zaś ich poszczególnych grup rodzajowych. Niemniej *derisking* może dotyczyć zwłaszcza podmiotów, z którymi należy zawsze łączyć wysokie ryzyko lub też które uzyskały taki status w ramach trwających dotychczas relacji z instytucją obowiązaną. Powstaje więc specyficzna sytuacja, wobec której instytucje obowiązane zamiast zarządzać ryzykiem podejmują decyzje o rozwiązaniu relacji z takim klientem. Pierwsza skala mieści się w przedsięwzięciach z zakresu AML/CFT i pozwala na nawet najtrudniejsze zarządzanie ryzykiem wobec klienta, druga zaś wiążę się z restrykcyjnym wykluczeniem finansowym. Należy zauważyć, że zarządzanie ryzykiem (zwłaszcza wysokim) może zakończyć się określonymi działaniami ze strony instytucji obowiązanej. Do nich należą, złożenie raportu SAR do jednostki analityki finansowej, ale także wstrzymanie transakcji, czy blokada środków na rachunku przy podejrzeniu związanym z możliwością udziału w procederze ML/FT. Nie jest to więc sytuacja bez wyjścia dla instytucji obowiązanej i daje ona możliwości większe niż wyłącznie zerwanie relacji z podmiotem obsługiwanym. Trudniejszym jest zaś sytuacja niedopuszczenia do relacji z instytucją obowiązaną, gdy nie zostanie ocenione indywidualne ryzyko klienta. Czyli w sytuacji, gdy proces oceny ryzyka nie zostanie podjęty, czy też zakończony w fazie przedumownej. W tej sytuacji instytucja obowiązana sama sobie nie daje możliwości rzeczywistej weryfikacji jakiejś ogólnej tezy o „powszechnym ryzyku" wywoływanym przed danego rodzaju klientów. Ten stan rzeczy może skomplikować także niemożność wprowadzenia danych o kliencie do bazy danych banku, w związku ze wstępnym rozpoznawaniem np. wniosku kredytowego, ale go negatywnym zweryfikowaniem (RODO). Negatywna weryfikacja może wynikać nie tylko z braku „zdolności kredytowej", ale także z podejrzeń decydenta banku, iż kredyt nie ma być elementem planowanego przedsięwzięcia gospodarczego, a kamuflażem procederu legalizacji środków pochodzących z czynu zabronionego. Brak możliwości pozostawienia takiego śladu w wewnętrznych bazach danych skutkuje także brakiem powstania elementów zbioru uczącego na potrzeby prowadzenia dalszych analiz. Rozwiązywaniem problemu *debankingu*, czy też odwrócenia co do myślenia o niedopuszczaniu do relacji klientów podwyższonego ryzyka nie sprzyja także niekiedy wdrożenie określonych rozwiązań prawnych. Przykładem jest tu art. 105a ust 1b w zw. z ust 1a ustawy prawo bankowe[13]. Dotyczy to w szczególności określenia na pozio-

[13] Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2022 r., poz. 2324, 2339, 2640, 2707; z 2023 r., poz. 180), zmiana wprowadzona ustawą z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu

mie ustawy (prawa bankowego) zamkniętego katalogu danych osobowych wykorzystywanych do profilowania w celu oceny zdolności kredytowej i analizy ryzyka kredytowego. Ograniczony katalog zmiennych wykorzystywanych w procesach kredytowych spowoduje obniżoną efektywność oceny ryzyka, szczególnie w przypadku nowych, nieznanych Klientów. W wyniku niższej efektywności modeli wzrośnie ryzyko kredytowe portfela, w związku z czym instytucje mogą ograniczyć akcję kredytową lub zaakceptują podwyższone ryzyko kredytowe, ale jego koszty będą musiały przenieść na kredytobiorców. Postulat dot. umieszczenia w Prawie bankowym przepisów określających katalog (kategorie) przetwarzanych danych osobowych w odniesieniu do zautomatyzowanego przetwarzania, w tym profilowania, z przyczyn obiektywnych może zostać spełniony jedynie poprzez wskazanie ogólnych kategorii danych, jakie podlegają profilowaniu, i to w sposób niewyczerpujący[14].

Jako przykład rozstrzygnięcia sądowego w zakresie „drogi wyjścia" poprzez wypowiedzenie umowy należałoby podać wyrok Sądu Najwyższego Nowej Zelandii, który rozstrzygał w sprawie E–Trans International Finance Ltd przeciwko Kiwibank Ltd.[15] Pozwany bank powiadomił powoda, że zmierza do zamknięcia rachunków w następstwie kontroli przeprowadzonej przez Zespół ds. Przestępczości Finansowej. Powód, E–Trans International Finance Ltd (E–Trans) prowadził działalność jako kantor wymiany walut i przekazów środków do i z Nowej Zelandii. Charakter prowadzonej przez nią działalności (transgraniczny przekaz środków) sprawiał, że E–Trans mogła być szczególnie podatna na próby przekazywania pieniędzy przez osoby trzecie za pośrednictwem jej rachunków; na przykład w celu ukrycia dochodów z przestępstwa lub uniknięcia wykrycia źródła finansowania terroryzmu. Aby prowadzić działalność jako podmiot przekazujący pieniądze z Nowej Zelandii, E–Trans potrzebował krajowego rachunku bankowego, który został założony w 2014 r., w Kiwibank Ltd. Komitet Wykonawczy ds. Ryzyka banku, zainicjował w 2015 r. politykę, zgodnie z którą bank będzie stopniowo „wyłączał" klientów, jako dostawców przekazów pieniężnych, których modele biznesowe nie będą zgodne z „apetytem na ryzyko" Kiwibanku, decyzja dotyczyła także niewchodzenia w relacje bankowe z nowymi klientami należącymi do tej kategorii. Strategią Kiwibanku Ltd. było podjęcie etapowego procesu rozwiązywania umów z odpowiednimi płatnikami. To stało się powodem, dla którego jej stosunki bankowe z E–Trans zostały zakończone dopie-

takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych (Dz. U. z 2019 r., poz. 730).

[14] T. B i a ł e k, ZBP krytycznie o projekcie ustawy sektorowej RODO, portal Bank.pl (dostępność 16 stycznia 2019 r.), (w:) https://bank.pl/zbp-krytycznie-o-projekcie-ustawy-sektorowej-rodo/.

[15] Wyrok z dnia 19 maja 2016 r. w sprawie CIV 2015-404-694, (w:) https://www.interest.co.nz/sites/default/files/embedded_images/E-Trans%20International%20Ltd%20v%20Kiwibank%20Ltd2%20%281%29.pdf.

ro w następnym roku. W konsekwencji podjęto czynności zmierzające do zamknięcia rachunku utworzonego dla E–Trans International Finance Ltd. W rezultacie prowadzonej rozprawy, wyrok zapadł na korzyść Kiwibank Ltd. w odniesieniu do każdego roszczenia.

Wobec powyższego należałoby się zastanowić, czy polityka bezpieczeństwa powinna opierać się na możliwym utrzymywaniu relacji z klientem, w stanie monitoringu wysokiego ryzyka np. związanego z finansowaniem terroryzmu, mając po temu wypracowane mechanizmy ocenne i obronne. Wszak instytucje obowiązane nie prowadzą czynności operacyjno-rozpoznawczych, których charakter i zakres pozwalałby na takie postępowanie (np. w ramach operacji specjalnej). Czy też „pozbywać się" problemu poprzez działania *debankingu* i *deriskingu*, a w rzeczywistości mnożąc ten problem sprowadzając ruch aktywów do nieuregulowanych kanałów przekazów pieniężnych o jeszcze wyższym ryzyku finansowania terroryzmu, nad którymi instytucje obowiązane a pośrednio także organy państwowe odpowiedzialne za bezpieczeństwo nie mają kontroli i możliwości bieżącego monitorowania. Tym samym pozbywając się jednego problemu, tworzą się następne, które można określić, iż są bardziej niebezpieczne od tych, których się pozornie „pozbyto". Wydaje się, że modele międzynarodowe AML/CFT, świadomie kreują w określonych obszarach instytucje obowiązane obarczając je określonymi rodzajami obowiązków na rzecz „strzeżenia" i identyfikowania zagrożeń. Ta „obowiązkowa misja" wiąże się z potrzebą szeroko rozumianego bezpieczeństwa gospodarczego, ekonomicznego i finansowego w poszczególnych krajach i w skali międzynarodowej. Filozofia określania tego typu podmiotów przede wszystkim opiera się na tym, aby za ich pośrednictwem i zaangażowaniem ustalać nośniki i ślady procederów prania pieniędzy oraz finansowania terroryzmu oraz identyfikować podejrzenia. *Debanking* i *derisking* są zdecydowanie czynnościami odwrócenia tych tez i świadomej deprecjacji systemu. Przedmiotowa postawa może być interpretowana jako wola niechęci wobec spełnienia misji bezpieczeństwa w systemie AML/CFT. Taka polityka bezpieczeństwa posiada także swoje przełożenia na inne kwestie. Związane są one z relacjami z krajami na obszarze, których w większości lub tylko działają nie-bankowe przepływy finansowe (np. niektóre kraje afrykańskie). Tego typu działalność w obszarze UE traktowana jest podejrzliwie, a w rzeczywistości jej proweniencja wynika z braku możliwości utworzenia na terytorium całego takiego państwa systemów klasycznej bankowości lub pozainternetowych systemów płatności. Ale także zubożeniem społecznym, wysokim poziomem przestępczości pospolitej, czy w większości przekazami realizowanymi na niskie kwoty. W konsekwencji tego typu pośrednicy lokalnego systemu finansowego mogą nie mieć dostępu do klasycznych banków europejskich, w kontekście przeciwdziałania ML/FT. A więc nie będzie możliwym założenie i prowadzenia dla wielu osób z diaspo-

ry ekonomicznej przebywających na terenie UE rachunków bankowych dla podmiotów organizujących możliwość przesyłu środków do kraju urodzenia/pochodzenia. Takie restrykcyjne podejście posiada negatywny wpływ ekonomiczny i społeczny na społeczności migrantów oraz krajów odbiorców. Utrata niedrogich i dostępnych przekazów pieniężnych może prowadzić również do mnożenia się nieformalnych kanałów przekazów pieniężnych bez nadzoru i stwarzać większe ryzyko finansowania terroryzmu[16].

W ramach UE przepisy wprost wskazują na prowadzenie polityki niedyskryminacji wobec podmiotów chcących założyć rachunek. Wynika to z art. 15 Dyrektywa (UE) 2014/92 w sprawie dostępu do rachunków płatniczych[17]. Państwa członkowskie zapewniają, by konsumenci legalnie przebywający w Unii nie byli dyskryminowani przez instytucje kredytowe ze względu na obywatelstwo lub miejsce zamieszkania lub z wszelkich innych powodów, o których mowa w art. 21 Karty[18], w przypadku gdy konsumenci ci ubiegają się o rachunek płatniczy na terytorium Unii lub korzystają z takiego rachunku. Warunki mające zastosowanie do posiadania podstawowego rachunku płatniczego nie mogą być w żaden sposób dyskryminujące[19]. Państwa członkowskie zapewniają, by podstawowe rachunki płatnicze były oferowane konsumentom przez wszystkie instytucje kredytowe lub wystarczającą ich liczbę, aby zagwarantować dostęp do tych rachunków wszystkim konsumentom na swym terytorium i zapobiegać zakłóceniom konkurencji (art. 16 ust. 1 dyrektywy 2014/92). Generalną zasadą jest, że państwa członkowskie UE zapewniają, by w sytuacji, gdy instytucja kredytowa rozwiązuje umowę dotyczącą podstawowego rachunku płatniczego z jednej lub więcej przyczyn wymienionych w ust. 2 lit. b), d) i e) oraz w ust. 3, poinformowała ona konsumenta o przyczynach i uzasadnieniu rozwiązania umowy na przynajmniej dwa miesiące, zanim to rozwiązanie stanie się skuteczne, w formie pisemnej i nieodpłatnie, chyba że przekazanie takiej informacji byłoby sprzeczne

[16] R. F u j i i - R a j a n i, Money Remitters Left Out in the Cold: Blanket De-Risking Policies, Counterterrorism and Government Intervention in New Zealand, Auckland University Law Review Vol 23 (2017), s. 234, (w:) http://www.austlii.edu.au/nz/journals/AukULawRw/2017/10.pdf.

[17] Dyrektywa Parlamentu Europejskiego i Rady 2014/92/UE z dnia 23 lipca 2014 r. w sprawie porównywalności opłat związanych z rachunkami płatniczymi, przenoszenia rachunku płatniczego oraz dostępu do podstawowego rachunku płatniczego Tekst mający znaczenie dla EOG, (w:) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32014L0092.

[18] Dotyczy Karty Praw Podstawowych Unii Europejskiej, art. 21 ust 1 - zakazana jest wszelka dyskryminacja w szczególności ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną.

[19] Rozdział IV, gdzie uplasowano ten przepis, ma zastosowanie do instytucji kredytowych. Państwa członkowskie mogą podjąć decyzję o stosowaniu rozdziału IV do dostawców usług płatniczych innych niż instytucje kredytowe. Oznacza to, że regulacja ta działa zawężająco.

z celami związanymi z bezpieczeństwem narodowym lub porządkiem publicznym. Poziom niedyskryminacji także powinna zapewniać dyrektywa 2015/2366[20]. W art. 36 stwierdza się, że państwa członkowskie zapewniają, by instytucje płatnicze miały dostęp do świadczonych przez instytucje kredytowe usług w zakresie rachunków płatniczych w oparciu o obiektywne, niedyskryminujące i proporcjonalne zasady. Taki dostęp powinien być wystarczająco szeroki, aby umożliwić instytucjom płatniczym świadczenie usług płatniczych w sposób wolny od przeszkód i efektywny. Jednocześnie wskazano na to, że instytucja kredytowa przekazuje właściwemu organowi należycie umotywowane uzasadnienie każdej odmowy. W przypadku odmowy uczestnik przekazuje dostawcy usług płatniczych, który zwrócił się do niego ze stosownym wnioskiem, pełne uzasadnienie takiej odmowy. Mimo przedmiotowych zapisów, to właśnie te konkretnie artykuły dyrektyw w ocenie EBA/ EUNB [21] mogły stać się przyczyną do radykalizacji zachowań wobec klientów.

Wydaje się, że stanem wyjściowym dla procederu *debankingu*, powinno być określenie „ryzyka" na jakie narażony jest dany podmiot wchodzący w relacje z podmiotem przez niego obsługiwanym ze względu na rodzaj prowadzonej działalności zawodowej. Dlatego też, równolegle do pojęcia *debankingu* funkcjonuje także określenie *deriskingu*. FATF w 2015 r. wskazał, że z *deriskingiem* mamy do czynienia w sytuacjach, w których finansowe instytucje zrywają lub ograniczają stosunki biznesowe z określonymi kategoriami klientów. Jest to podejście raczej statyczne związane z założoną organiczną i zbudowaną na skrajności oceny „identyfikacją" ryzyka. Przy czym jedynym przyczynkiem do *deriskingu/debankingu* jest założenie nieobsługiwania określonych podmiotów (np. zajmujących się obrotem kryptowalutą), osób fizycznych, czy firm pochodzących z określonych państw lub niekorzystanie z banków-korespondentów mających siedzibę w tzw. obszarach *offshore*/rajach podatkowych. Drugie podejście wiąże się zwłaszcza z dynamicznym podejmowaniem działań. Ma to miejsce w zakresie tzw. zarządzania ryzykiem (monitoring klienta, transakcji), bądź też alternatywnie do niedopuszczenia do jego wystąpienia, ale także ze skrajną reakcją na ryzyko, którego wartość negatywna przekracza określony w danej instytucji pułap bezpieczeństwa (apetytu na ryzyko). Ta skraja reakcja może mieć swoje źródła w nieproporcjonalnych kosztach obsługi ryzyka w porównaniu z decyzją o odmowie obsługi podmiotów je generujących (zwłaszcza tych, które od początku relacji z instytucją musiałyby być zakwalifikowane do potrzeby sto-

[20] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG), (w:) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32015L2366.

[21] European Banking Authority, Europejski Urząd Nadzoru Bankowego.

sowania wzmożonych środków bezpieczeństwa finansowego). Banki będące respondentami, które doprowadziły do zaprzestania odpowiednich relacji korespondenckich, twierdziły, że decyzje te zostały podjęte w celu zakończenia relacji biznesowych i były oparte na pewnych cechach (np. banki działały w jurysdykcjach wysokiego ryzyka lub jurysdykcjach znajdujących się na szarej liście FATF) niezależnie od indywidualnych wysiłków banków w zakresie AML/CFT[22]. Z pewnością zakres reakcji na ryzyko będzie różnorodny, uzależniony od potencjału instytucji, jego wielkości czy rodzaju zidentyfikowanego ryzyka. Działania identyfikujące i oceniające ryzyko instytucjonalne powinny być proporcjonalne do charakteru i wielkości instytucji obowiązanej. Natomiast w odniesieniu do ryzyka indywidualnego z chwilą jego oceny jako wysokiego instytucja musi podjąć adekwatne, niekiedy kosztowne środki zaradcze. Tym samym instytucja obowiązana nie powinna mieć zarówno w zakresie faktycznym, jak i prawnym „związanych rąk" wobec możliwości budowania oceny identyfikacji, weryfikacji i monitoringu potencjalnego lub posiadanego klienta w aspekcie oceny ryzyka. Inaczej nie będzie się ona starała podjąć to ryzyko i rozpocząć lub kontynuować relacje z klientem (zarządzać ryzykiem). Radykalne rozwiązania jednak w takim przypadku związane są z przewyższeniem kosztów obsługi niż ustalone i planowane lub też są one wynikiem braku możliwości organizacyjnych/kadrowych do obsługi klientów tak wysokiego ryzyka. Niekiedy jednak tego rodzaju rozwiązania mogą być krzywdzące dla klientów np. w przypadku organizacji charytatywnych, jako NGO[23], które realizują się na terenach państw podwyższonego ryzyka ML/FT lub innego (ich charakter może dopuszczać je jako jedyne organizacje, które mogą działać w takich terenach). Efektem negatywnym może być także opóźnienie pomocy charytatywnej lub wręcz zaniechanie programów wsparcia dla lokalnej społeczności[24]. Do skrajnych przeciwdziałań wyprzedzających „ocenę ryzyka" zgodnie z modelem przyjętym dla AML/CFT, zaliczymy zarówno *debanking*, jak i *demarketing*. *Derisking*, jest także działaniem skrajnym, ale także zależnym od czasokresu wykrycia zagrożenia. Ponadto te skrajne podejścia mieszczą się w zakresie unikania ryzyka – ma ono charakter zabezpieczający, prewencyjny i polega na zaniechaniu działań, które mogą być ryzykowne. Poszczególne programy AML/CFT różnią się między sobą w zależności od rodzaju instytucji, ponieważ poziom ryzyka i rozumienie ryzyka przez każdą po-

[22] W obszarach, gdzie instytucje obowiązane przyjmują sektorowe podejście do zmniejszania ryzyka, mają tendencję do kończenia relacji z rodzajowymi klientami i klientami o wyższym ryzyku, takimi jak banki korespondentów zagranicznych (FCB), czy firmy świadczące usługi pieniężne (MSB).

[23] Skrót od ang. *non-governmental organization*, organizacja pozarządowa.

[24] Niestety wielokrotnie tego rodzaju organizowana pomoc była powodem do konfiskaty przekazanych produktów, nielegalnym ich handlem nie tylko przez terrorystów, członków grup przestępczych, ale także przez miejscowe reżimy kontrolujące kraj.

szczególną instytucję obowiązaną, nie są takie same. *Derisking* można również uznać za strategię, którą mogą wdrożyć te organizacje, które nie są już w stanie zarządzać kolejnym ryzykiem związanym z praniem pieniędzy. Wobec wielości i różnorodności ryzyk na jakie narażony jest podmiot (np. przedsiębiorstwo)[25]. Jest to każe postępowanie w kategorii zabezpieczenia się (przed nałożeniem ew. kary administracyjnej) wobec organów kontrolnych w zakresie oceny zgodności realizacji zadań z obowiązkami wynikającymi z np. ustawy o p.p.p.f.t. Wskazane odnoszą się zwłaszcza do klienta postrzeganego jako osoba prawna lub fizyczna. O ile w określonych rodzajach relacji podmiot może odmówić wejścia w stosunki prawne, handlowe, logistyczne z danym kontrahentem, i nie mają one większego znaczenia w gospodarce wolnorynkowej, w związku z możliwością poszukania innego partnera gospodarczego, to w innych przypadkach zwłaszcza, gdy są one naznaczone prawnie (np. dotyczą sankcji, relacji z PEP) mogą być one bardzo dolegliwe wobec klienta nieznajdującego adekwatnego partnera gospodarczego, finansowego wobec potrzeby realizowania własnych interesów gospodarczych. Jako jeden z czynników zajęcia się ryzykiem w celu jego identyfikacji oceny i monitoringu a nie *ab initio* zerwaniem lub niedopuszczeniem do podjęcia relacji jest presja instytucji kontroli i nadzoru w ramach systemu AML/CFT. System ten jedynie wyjątkowo i to po niemożności zrealizowania określonych obowiązków przez instytucję obowiązaną, pozwala na podobne działania. W rzeczywistości może dojść do sytuacji, gdy mimo braku pozytywnej oceny w samej instytucji, ta będzie musiała swoim kosztem realizować politykę AML/CFT wywołaną decyzjami organów nadzorczych. Sytuacja powodów do zastosowania *debankingu* czy *deriskingu* nie jest jednoznaczna. O ile można doszukiwać się uzasadnienia takich poczynań z chwilą ustalenia, że dany podmiot jest utworzony lub przejęty przez osoby związane z finansowaniem działań terrorystycznych i instytucja obowiązana podejmie decyzję o ich nieobsługiwaniu. Ta sytuacja nie jest jednoznaczna, gdy relacje korespondenckie czy też podmioty posiadają siedzibę w określonych krajach/strefach jako *off-shore*/rajach podatkowych. Z tego typu rozwiązań korzystają zarówno podmioty powiązane z terroryzmem, politycznymi reżimami, wywołujące konflikty zbrojne wbrew stanowisku wspólnoty międzynarodowej, czy podmioty związane z przestępczością kryminalną. narkotykową lub w celu unikania opodatkowania. Niemniej z tego typu obszarów korzystają także realnie działające podmioty gospodarcze, inne instytucje finansowe, są one podstawą do rozliczeń przy formowaniu (w ramach swobody) umów handlowych. Z pewnością natomiast, zdając sobie sprawę z tego, jak wykorzystywane są jurysdykcje tych obszarów, są one czynnikiem ryzykogennym i jednocześnie kryminogennym w ramach oceny ryzyka

[25] Ryzyka związane z: dostawami, finansowaniem, zatorami płatniczymi, jakością kadry itp.

AML/CFT (walor ten może być oceniany jako obszar geograficzny, wobec wyceny skali ryzyka instytucjonalnego i indywidualnego). Radykalne postępowanie z takimi obszarami zmierza do wykluczenia ich z globalnego świata systemu finansowego. Kwestię ewentualnego ujednolicenia schematów postępowania można byłoby rozpatrywać wobec ustanowienia jednolitych standardów regulacyjnych i nadzorczych nie tylko dla obszaru ML/FT, ale dla całości działań instytucji obowiązanych. Stąd też kluczowa rola w tym zakresie pozostaje takich instytucji, jak: Komitet Bazylejski (ponadnarodowo), czy UKNF (krajowo)[26].

Niestety wobec *deriskingu* i *debankingu* można więc wymienić szereg negatywnych zachowań jakie generują tego rodzaju postępowania w obszarze AML/CFT. Do takich negatywnych efektów zaliczymy:

– kiedy relacje z klientami są zakończone, zapotrzebowanie tych klientów na usługi finansowe pozostaje. Jeśli klienci ci, nie są w stanie uzyskać dostępu do usług większych dostawców, mogą przenieść się do banków z mniej rygorystycznymi kontrolami AML. Banki te mogą nie być świadome lub nie być w stanie bezpiecznie zarządzać ryzykiem związanym z praniem pieniędzy, jakie stwarzają niektórzy klienci.
– kiedy bank kończy współpracę w celu ograniczenia ryzyka, klienci mogą po prostu wrócić do banku, korzystając z innego wektora biznesowego.
– ograniczanie ryzyka często niweczy ostateczne cele programów AML/CFT, którymi są wymiana informacji i ograniczanie przestępczości, ponieważ praktyki te spychają organizacje przestępcze na mniej uregulowane terytorium, gdzie ich monitorowanie staje się trudniejsze;
– zmniejszenie ryzyka przez kilka banków w całych sektorach może mieć znaczący wpływ na system finansowy. To zbiorowe działanie może również stwarzać pozory działania banków w zmowie, a tym samym generować potencjalne konsekwencje prawne;
– w niektórych przypadkach zmniejszanie ryzyka związanego z przeciwdziałaniem praniu pieniędzy kończy się szkodą dla organizacji humanitarnych lub organizacji charytatywnych, które polegają na określonych usługach finansowych, aby uzyskać dostawy i inne rodzaje krytycznej pomocy dla osób znajdujących się w trudnej sytuacji w krajach rozwijających się[27].

W styczniu 2022 r. Europejski Urząd Nadzoru Bankowego (EUNB) opublikował swoją opinię w sprawie skali i skutków ograniczania ryzyka w UE oraz kroków, jakie powinny podjąć właściwe organy w celu rozwiązania problemu nieuzasadnionego ograniczania ryzyka. Stwierdzono w nim, że *derisking* odnosi się do decyzji instytucji finansowych o nieświadczeniu usług

[26] Zob. M. G. Williams, De-Risking/De-Banking “The Reality Facing Caribbean Financial Institutions”, s. 9.

[27] De-Risking AML – Strategies and Alternatives, July 2022[w] https://complyadvantage.com/insights/de-risking-aml/.

klientom w określonych kategoriach ryzyka. Ograniczanie ryzyka może być uzasadnionym narzędziem zarządzania ryzykiem, ale może też być oznaką nieskutecznego zarządzania ryzykiem związanym z praniem pieniędzy i finansowaniem terroryzmu, co czasami ma poważne konsekwencje. Aby ocenić skalę i wpływ ograniczania ryzyka w całej UE oraz lepiej zrozumieć, dlaczego instytucje decydują się na ograniczanie ryzyka określonych kategorii klientów zamiast zarządzać ryzykiem związanym z takimi relacjami[28]. W dokumencie zaproponowano, aby wspólnie EUNB, AMLA[29] i Komisja UE przygotowały wytyczne, które mógłby wyjaśnić, w jakich sytuacjach konto z podstawowymi funkcjami powinno zostać odrzucone lub zamknięte, lub też jego podstawowe funkcje mogły zostać ograniczone.

FATF, ograniczając kwestie do spraw związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu posługuje się określeniem *derisking* co posiada swoje umotywowanie w analizie ryzyka instytucjonalnego i indywidualnego, w postaci jego identyfikacji i oceny. Ten zakres należy do obowiązków wykonywanych przez instytucje obowiązane w ramach systemu AML/CFT[30]. Główne podejście FATF do zmniejszania ryzyka opiera się na zaleceniach kreowanych przez tą organizację. W rezultacie wymaga ono od instytucji finansowych identyfikacji, zrozumienia, oceny i wdrożenia środków przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu współmiernych do zidentyfikowanych zagrożeń. Pojęcie *deriskingu* posiada znacznie szerszy zakres niż określenie *debankingu* ze względu na to, że zbiór instytucji obowiązanych dotyczy nie tylko instytucji wykonujących czynności bankowe. Pojęcie *debankingu* może, ale nie musi być częścią systemu przeciwdziałania ML/FT. Odmówienie prowadzenia konta bankowego czy określonych usług przez banki może wynikać także z innych powodów niż określonych dla sytuacji związanych z przeciwdziałaniem praniu pieniędzy, czy finansowaniu terroryzmu. FATF rozumie termin *derisking* jako oznaczający sytuację, w których instytucje finansowe zrywają lub ograniczają relacje biznesowe z całością krajów lub grup klientów w celu uniknięcia ryzyka, a nie zarządzania nim zgodnie z celem stawianym przez FATF tj. podejściem opartym na ryzyku (RBA). Takie podejście stanowi poważny problem dla FATF i innych regionalnych organizacji w zakresie, w jakim usuwanie ryzyka może kierować transakcje finansowe do mniej/nieuregulowanych kanałów zmniejszając przejrzystość przepływów finansowych i tworząc wyklucze-

[28] EBA alerts on the detrimental impact of unwarranted de-risking and ineffective management of money laundering and terrorist financing risks oraz Opinion of the European Banking Authority on 'de-risking', (w:) https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf.

[29] The Anti-Money Laundering Authority of the European Union.

[30] FATF GUIDANCE CORRESPONDENT BANKING SERVICES OCTOBER 2016, (w:) file:///C:/Users/HP/Downloads/Guidance-Correspondent-Banking-Services.pdf.

nie finansowe, zwiększając tym samym narażenie na ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu[31]. Z przesyłanych w ramach badania FATF, ankiet informacyjnych wynikało, że w niektórych przypadkach banki wycofywały się ze współpracy wyłącznie na podstawie tzw. zysków („*de-marketing*"), niezależnie od kontekstu ryzyka i warunków rynkowych. Zalecenia wymagają, aby instytucje finansowe identyfikowały, oceniały i rozumiały ryzyko związane z praniem pieniędzy/finansowaniem terroryzmu, oraz wdrożyły środki AML/CFT, które są współmierne do zidentyfikowanego ryzyka. Należy zwrócić uwagę na to, że taktyka pozyskania wiedzy o ryzyku, jego identyfikacja i ocena, nawet w najbardziej skrajnych kategoriach zagrożenia, pozwala na ocenę niebezpieczeństwa i ustalenia schematu postępowania z nim. Taki stan rzeczy umożliwia jego kontrolowanie, ale także poszukiwanie nowych rozwiązań, jak skutecznie takiemu ryzyku przeciwdziałać i go monitorować. W konsekwencji takie patrzenie na ryzyko wobec czynności *debankingu* stawia możliwości o dziwo „pozytywnej" oceny schematów „prania pieniędzy" jako legalizacji aktywów za pośrednictwem formalnych schematów finansowych. Ryzyko regulacyjne wynikające z obsługi jurysdykcji wysokiego ryzyka, które grozi odcięciem tych jurysdykcji od globalnej sieci finansowej, stwarza poważne warunki do większej przestępczości finansowej. Zwłaszcza odejścia od korzystania ze schematów (w miarę identyfikowalnych) podmiotów nadzorowanych na rzecz niekontrolowanej w większości przestrzeni czarnej i szarej strefy gospodarczej i finansowej (tworzenie warunków dla większej przestępczości finansowej niż może być ona w jakiś sposób kontrolowana) chrakteryzującymi się nieprzewidywalnymi i zmiennymi w czasie schematami. Na kwestie te zwrócił także uwagę raport EBA, ESMA, EIOPA wskazując, że ryzyka prania pieniędzy/finansowania terroryzmu wynikają między innymi z tego, że transakcje wysokiego ryzyka są spychane do podziemia, ponieważ firmy wycofują się z oferowania usług dla mniej rentownych klientów, które wiążą się z wyższym ryzykiem ML/TF[32]. Innym negatywnym skutkiem *deriskingu*/*debankingu* może być zdominowanie podmiotów finansowych jako mających status instytucji obowiązanych (ich przejęcie) przez beneficjentów powiązanych ze zorganizowaną przestępczością kryminalną czy organizacjami terrorystycznymi.

Rozwiązanie, które stanowi uzasadnienie dla metod opartych na ryzyku stosowanych obecnie do zwalczania prania pieniędzy i finansowania terroryzmu, może spowodować poważny konflikt między organami regulacyjnymi a nadzorowanymi przez nich podmiotami. Wynika to z faktu, że przyznanie instytucjom obowiązanym swobody w tworzeniu własnych zasad przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oznacza również więk-

[31] *Ibidem*, s. 4.

[32] Raport EBA, ESMA, EIOPA, Joint Opinion, on the risks of money laundering and terrorist financing affecting the Union's financial sector, 20 February 2017, s. 6.

sze prawdopodobieństwo różnic w interpretacji i osądach – sytuacji, która naraża instytucje na znaczne niebezpieczeństwo, jeśli nie zastosują one prawidłowo podejścia opartego na ryzyku do ich spraw. Straty finansowe i wizerunkowe wynikające z takich niepowodzeń mogą być kosztowne[33]. Niektóre z instytucji obowiązanych nie mają infrastruktury, aby wesprzeć dodatkowy poziom należytej staranności potrzebnej na rynkach wysokiego ryzyka lub po próbach dochodzą do wniosku, że ryzyko nie jest tego warte, i tym samym ograniczanie swojej działalność na tych rynkach lub nawet całkowite z nich wyjście staje się dla nich jedynym rozsądnym rozwiązaniem. Każdy kraj styka się zarówno z wielością instytucji obowiązanych, różnorodnie przygotowanych na reagowanie na ryzyko, ale także z wielością ryzyk, które można kwalifikować jako wysokie. Brak stabilności bezpieczeństwa, wymuszone migracje, rozwój przestępczości zorganizowanej, klęski żywiołowe, szeroki zasięg epidemii, czy trwające konflikty zbrojne ułatwiają powstawanie ryzyk, które należałoby zakwalifikować do najwyższej kategorii zagrożenia. Mnożąc to przez wielość instytucji obowiązanych można uzyskać poważny wynik zagrożenia, wobec niektórych z nich, które będą korzystały z elementów *debankingu*, czy *deriskingu*. A to już prosta droga do rozbudowy podziemnej bankowości i paralelnych instrumentów i kanałów przepływów środków finansowych. W konsekwencji użycie opcji odstąpienia lub nieobsługiwania określonych podmiotów, stanowi opcję krótkoterminowego „sukcesu" (ocenianego bardzo osobiście/subiektywnie), który w dłuższym okresie może jedynie pogorszyć stan bezpieczeństwa finansowego (ocenianego globalnie). Co możliwe, z czasem *debanking*, czy *derisking* może stać się jednym z czynników identyfikacji i oceny ryzyka AML/CFT. Uwzględniając, że ryzyko ML/FT jest tylko częścią ryzyk, z którymi może się borykać instytucja obowiązana w ramach wewnętrznych polityk oraz działań *compliance*, taka instytucja – o ile jest to prawnie i realnie możliwe – musi ocenić wszystkie rodzaje ryzyk globalnie. Zwłaszcza te, które mieszczą się w innych kategoriach, jak prawo, marketing, prestiż na rynku, konkurencja, które także mogą wpływać na kształt identyfikacji i oceny ryzyka ML/FT. Zwłaszcza gdy dyskwalifikująca w ocenie innych działów instytucji a oceniona pozytywne polityka całościowego bezpieczeństwa nie zważa na mechanizmy oceny i monitoringu przedmiotowego ryzyka w całkiem innych obszarach aktywności zawodowej instytucji obowiązanych (brak holistycznej oceny ryzyk). Szczególnie negatywny wpływ *deriskingu* może wywrzeć na działania związane z przeciwdziałaniem finansowaniu terroryzmu. W przeciwieństwie do AML, CFT wiąże się to nie tylko z pozyskiwaniem środków w sposób przestępczy, ale także z legalnych źródeł, które skierowane zostają do przestępczego działania.

[33] M. Nilsson, E. Shorrock, *Debanking* and the Law of Unintended Consequences, (w:) https://www.kroll.com/en/insights/publications/financial-compliance-regulation/global-regulatory-outlook-2019/*debanking*-and-the-law-of-unintended-consequences.

W konsekwencji zastosowanie *derisking/debanking-u* może spowodować „nierozpoczęcie" obserwacji śladu początkowego łańcucha dostaw aktywów dla terrorystów. ale także ograniczyć możliwości śledzenia środków bliższych wykorzystaniu czy redystrybucji wokół samej organizacji zamachów terrorystycznych. Tym samym, co nie będzie widocznym dla działań operacyjnych, traci się wiedzę o pośrednich, początkowych i docelowych śladach transakcyjnych procederu finansowania zamachów. Poprzez takie niekonsekwentne poczynania instytucji obowiązanych następuje utrata wiedzy o możliwości śledzenia środków oraz wykorzystania śladu transakcyjnego na potrzeby analizy kryminalistycznej zawiązanej o identyfikacją kryminalnych sieci przestępczych czy terrorystycznych. Należy zauważyć, że w ocenie ryzyka liczy się zwłaszcza jego identyfikacja, ocena i monitoring oraz właściwe czasowo ujawnienie nieprawidłowości związanych z podejrzeniem udziału klienta w procederze ML/FT. Takie podejście ma także wpływ na rozwój już stosowanych paralelnych kanałów przepływów aktywów dla beneficjentów terrorystycznych, które można ujmować jedynie przy wykorzystaniu metod operacyjno-rozpoznawczych. Nie będą one widoczne jako efekty monitoringu stosowanego przez instytucje obowiązane w ramach rozpoznania analitycznego.

Wszystkie przedstawione zachowania w postaci: *debankingu*, *demarketingu*, czy *deriskingu*, posiadają część wspólną polegającą na tym, że instytucja obowiązana (inny podmiot), wypowiada dotychczasowe relacje lub nie nawiązuje nowych z podmiotem obsługiwanym. Ten określony rodzaj zachowania umotywowany jest różnymi czynnikami. Czynniki te można ogólne określić jako wywołane ryzykiem zbyt dużym wobec bezpieczeństwa samej instytucji, powiązań przestępczych, sankcyjnych, czy mogących zaszkodzić statusowi komercyjnemu (marketingowemu) danej instytucji świadczącej produkty i usługi wobec takiego klienta. Tego rodzaju zachowania można traktować bardzo szeroko wobec jedynie określonego wycinka – podejścia opartego na ryzyku, które reprezentuje FATF. Sposób budowania „odmowy" obsługi klienta, przyjmując za podstawę wytyczne FATF może być realizowany z określonych powodów i w określony sposób. Odejście FATF do „zmniejszania ryzyka" opiera się na Zaleceniach FATF, które wymagają od instytucji finansowych identyfikacji, oceny i zrozumienia ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu oraz wdrożenia środków przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, które są współmierne do zidentyfikowanego ryzyka[34]. Takie podejście oczywiście nie wyklucza podjęcia skrajnych czynności odmowy obsługi klienta, niemniej musi się to łączyć przede wszystkim, z: 1. niemożliwością ustalenia prawdopodobieństwa skali ryzyka 2. odmową udziału klienta w identyfikacji tego

[34] FATF, Drivers for "de-risking" go beyond anti-money laundering / terrorist financing, (w:) https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/derisking-goes-beyond-amlcft.html.

ryzyka oraz 3. niemożnością zastosowania środków bezpieczeństwa finansowego w indywidualnej sprawie. Najwięcej kontrowersji dotyczy nie tylko bezpośrednich relacji z klientem, ale także realizowania zleceń wykonywanych za pośrednictwem banków-korespondentów. Przy ocenie ryzyka ML/TF, krajowe właściwe organy i instytucje finansowe powinny analizować i starać się zrozumieć, w jaki sposób identyfikowane przez nich zagrożenia związane z praniem pieniędzy i finansowaniem terroryzmu wpływają na nie. Ocena ryzyka stanowi zatem podstawę do stosowania środków AML/CFT z uwzględnieniem tego ryzyka. Kwestie te związane są zarówno z zakresem podmiotowych instytucji obowiązanych, które oceniają ryzyko ML/FT, jak i z zakresem przedmiotowym oceny i dostosowania go do własnych ocen ryzyka realizowanych w tych poszczególnych instytucjach. Innym zagadnieniem jest reagowanie na uzyskaną skalę ryzyka poprzez odpowiednie (adekwatne) stosowanie działań zapobiegawczych, zwłaszcza poprzez stosowanie mitygantów (przy ryzyku instytucjonalnym) oraz środków bezpieczeństwa finansowego (wobec ryzyka indywidulanego). Dotyczy to takich elementów, jak: rodzaju, stopnia, częstotliwości, intensywności. Bankom można przyznać elastyczność w decydowaniu o najskuteczniejszym sposobie radzenia sobie z innymi rodzajami ryzyka, w tym tymi, które zostały zidentyfikowane w krajowej ocenie ryzyka (KOR) lub przez same banki. Strategia mająca na celu ograniczenie tych zagrożeń musi uwzględniać obowiązujące krajowe przepisy prawne, regulacyjne i ramy nadzorcze. Przy podejmowaniu decyzji, w jakim stopniu banki są w stanie zdecydować, w jaki sposób ograniczać ryzyko, kraje powinny rozważyć między innymi zdolność swojego sektora bankowego do skutecznego działania w zakresie identyfikowania i zarządzania ryzykiem ML/TF. Istotnym jest także ustalanie i wykorzystywanie informacji pozwalających na identyfikację ryzyka. Ocena ryzyka prania pieniędzy i finansowania terroryzmu wykracza zatem poza zwykłe gromadzenie informacji ilościowych i jakościowych: stanowi także podstawę do efektywnego ocenienia skali ryzyka ML/TF łagodzenia skutków i powinna być modyfikowana, aby zachować aktualność[35]. Uwagi te odnoszą się także do innego rodzaju instytucji obowiązanych. Zasady dotyczą także relacji utrzymywanych z innymi bankami. Instytucje obowiązane mogą zdecydować, aby przy podejściu opartym na ryzyku, rozszerzyć je także na wszystkie relacje korespondencyjne, które utrzymują np. z finansowymi podmiotami niebankowymi czy dostawcami usług płatniczych.

Niestety *debanking*, czy *derisking* to także wynik umożliwiania przez podmioty nadzorcze prowadzenia własnych polityk bezpieczeństwa w instytucjach obowiązanych (nadzorowanych). W warunkach ustawy o p.p.p.f.t

[35] FATF, GUIDANCE FOR A RISK-BASED APPROACH THE BANKING SECTOR, OCTOBER 2014, s.9, (w:) file:///C:/Users/HP/Downloads/Risk-Based-Approach-Banking-Sector.pdf.

wskazano, że: implementując art. 8 dyrektywy 2015/849, zobowiązano instytucje obowiązane do podjęcia odpowiednich działań w celu zidentyfikowania i ocenienia ich ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu (art. 27 ust. 1). Przy sporządzaniu tej oceny instytucje obowiązane mogą posiłkować się KOR, jak również sprawozdaniem Komisji Europejskiej z ponadnarodowej oceny ryzyka prania pieniędzy oraz finansowania terroryzmu (art. 27 ust. 2)[36]. Sam art. 8 dyrektywy 2015/849 wskazuje na to, że: państwa członkowskie zapewniają podjęcie przez podmioty zobowiązane odpowiednich działań w celu zidentyfikowania i ocenienia ich ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, z uwzględnieniem czynników ryzyka obejmujących ryzyko dotyczące klientów, państw lub obszarów geograficznych, produktów, usług, transakcji lub kanałów dostaw. Działania te są proporcjonalne do charakteru i wielkości podmiotów zobowiązanych. Inicjatywa więc identyfikacji i oceny ryzyka instytucjonalnego musi wyjść od instytucji obowiązanej a nie od podmiotu nadzorczego. Ustawodawca także powinien głównie ustalić ramy, w których będzie funkcjonowała instytucja na potrzeby zbudowania własnej oceny ryzyka. Układ, który stanowi uzasadnienie dla opartych na ryzyku metodach stosowanych obecnie do zwalczania prania pieniędzy i finansowania terroryzmu, może potencjalnie wywołać poważny konflikt między organami regulacyjnymi a podmiotami, które nadzorują. To dlatego, że daje instytucji swobodę tworzenia własnych polityk AML/CFT oznacza to również, że istnieje większe prawdopodobieństwo różnic w interpretacji i osądach – sytuacji, która naraża instytucje na poważne niebezpieczeństwo, jeśli nie zastosują prawidłowo metody opartej na ryzyku przy podejściu do ich biznesu[37]. Wyzwaniem staje się więc zarządzanie ryzykiem wobec zwykłego zamykania rachunków dla klientów (lub ich nieotwierania). Innym rozwiązaniem jest samoograniczenie się na rynku usług i inwestycji świadomie ograniczając swoje relacje jedynie do określonych, wytypowanych i znanych podmiotów-klientów.

Z powyższego wynika, że mając na uwadze określone ryzyka zachowania instytucji obowiązanych są obowiązkowe, dopuszczalne lub wykraczające poza zakres racjonalnego postępowania z ryzykiem. Wyznacznikiem tych dopuszczalnych i samoistnie kreowanych reguł postępowania są zarówno regulacje generalne, jak i lokalna lub indywidualna polityka bezpieczeństwa samych instytucji obowiązanych. Tym samym odpowiedzialna za kreowanie polityk, standardów *compliance* i bezpieczeństwo instytucji kadra wyższego szczebla, powinna mieć stały dostęp do informacji, analiz i ocen ryzyka, w tym

[36] Uzasadnienie do rządowego projektu ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, druk sejmowy nr 2233 Sejmu VIII Kadencji, s. 19, (w:) https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2233.

[37] Global Regulatory Outlook 2019, (w:) https://www.kroll.com/-/media/assets/pdfs/publications/compliance-and-regulatory-consulting/global-regulatory-outlook-2019.pdf.

zwłaszcza instytucjonalnego na potrzeby równoważenia zachowań instytucji wobec zewnętrznych czynników ryzyka. W rzeczywistości mogą wystąpić dwa niebezpieczne kierunki rozwiązań. Pierwszy skupiony na pro-omijaniu zagrożenia i ryzyka wiązanego z ML/FT poprzez niedopuszczanie do obsługi i bycia klientem instytucji obowiązanych. Drugi zaś, skupiający się na realizowaniu relacji, ale bez skuteczności oceny jej ryzyka i niesionego zagrożenia. Przerwaniem tej drugiej sytuacji może być wynikiem dokonania ustaleń kontrolnych przez podmioty nadzorcze jako niepodejmowania obowiązków wynikających z treści przepisów regulujących sprawy związane z AML/CFT. W pierwszym przypadku mamy do czynienia z nierealizowaniem sprawy, w drugim z niezałatwieniem sprawy. Należy zaznaczyć, że instytucje obowiązane stanowią niejako „sieć" zarzuconą na potencjalnych sprawców przestępstw prania pieniędzy czy finansowania terroryzmu, ale także przestępstw źródłowych i docelowego przeznaczania środków na rzecz terrorystów. Alternatywne działania prowadzone przez uprawnione organy w drodze czynności operacyjno-rozpoznawczych nie uzyskają tak szerokiego rozpoznania jakie daje relacja z klientem, oraz systematyczne jego monitorowanie. Rezygnacja z tych działań może być podejmowana jedynie w wyjątkowych przepadkach i to w oparciu o przepisy prawa regulacji sektorowych. Zbyt subiektywne podejście do identyfikacji i oceny ryzyka w instytucji obowiązanej może zakończyć się postępowaniem mającymi charakter *debankingu* i *deriskingu*. Niestety wraz ze zmianą podejścia do zagrożenia ML/FT z podejścia opartego na regułach i przejście na podejście oparte na ryzyku nie wyzbyto się wielu problemów. Jednym z nich jest wskazany *debanking* i *derisking,* czyli postępowanie w celu uniknięcia problemów poprzez niedopuszczanie do zadziałania sytemu AML/CFT (nie licząc wyjątków). Innym jest mała wydajność informacji przesyłanych z instytucji obowiązanych do jednostek krajowych analityki finansowej. Realizowane jest to poprzez przesyłanie raportów z nieefektywnych lub fałszywych alarmów tzw. „czerwonych flag". Jest to więc wyszukiwanie anomalii podejrzalności w mniej niebezpiecznych obszarach niż w tych, jakie typowane są do źródeł podejrzalności w zakresie aktywności sprawców ML/FT. W konsekwencji jednostki analityki finansowej otrzymują niepełny obraz zagrożenia sięgający w obszar „*inadequate crime*"[38]. Jest to możliwy wynik tego, że te „twarde obszary" zagrożenia zostały przedwstępnie wyeliminowane poprzez zastosowanie *deriskingu.* Odstępowanie od obsługi klienta pozostaje jednak zrozumiałym, ponieważ przy jego wczesnej, a nawet pre-relacyjnej negatywnej identyfikacji występuje obawa, że może przyczynić się on do działania na szkodę instytucji, innych klientów i doprowadzić do negatywnej społecznej oceny instytucji (reputacja inwestycji, brak stabilności i przejrzystości działań

[38] „Nieadekwatna przestępczość" to efekt w postaci rodzaju ustalonej przestępczości (jej symptomów), jako wyniku rozpoznawania jej w sposób nieodpowiadający i niezgodny wobec właściwych kierunków jej zwalczania.

może „odstraszyć" dużych inwestorów zachowujących dystans wobec zagrożenia aktywowanego kapitału). Taki efekt może mieć swoje gospodarcze i finansowe uzasadnienie. Niestety radykalna reakcja instytucji obowiązanych poprzez zastosowanie *debankingu*, czy *deriskingu* wiąże się także ze słabym przygotowaniem pracowników i kadry nadzorczej do pracy nad kwestiami ryzyka zarówno instytucjonalnego, jak i indywidualnego. Instytucje nie rozumieją jak z ich produktem łączy się ryzyko, nie posiadają właściwego przygotowania merytorycznego do podejmowania decyzji w obszarze *compliance*, co może być wynikiem braku kierunkowych szkoleń i właściwie przygotowanej wewnętrznej analizy ryzyka i poszukania mitygantów oraz kierunkowania środków bezpieczeństwa wobec profilu klienta. Ten stan doprowadza do decyzji, iż podjęcie radykalnego rozstrzygnięcia wydaje się działaniem najwłaściwszym (obronnym). Zwłaszcza, że zawsze można przytoczyć argumenty w zakresie kosztów obsługi klienta wyższego ryzyka czy skuteczności (wobec instytucji i innych klientów) takiego postępowania. Ponadto zawsze pozostaje także aktualna kwestia braku zaangażowania kierownictwa wyższego szczebla, w szczególności w połączeniu z kulturą korporacyjną, które dąży do osiągnięcia zysków kosztem solidnej zgodności. Ten stan może stanąć na przeszkodzie wobec skutecznego systemu i kontroli AML/CFT. Często towarzyszy im niski poziom zgodność z politykami i procedurami AML/CFT, które pozostają niekwestionowane, chrakteryzującą się niechęcią postawy, reprezentowaną przez kierownictwo wyższego szczebla, do wzięcia odpowiedzialności za ryzyko związane z praniem pieniędzy/finansowaniem terroryzmu, na przykład w odniesieniu do *onboardingu* klientów szczególnie wysokiego ryzyka[39]. Przeszkodą do uzyskania właściwej oceny ryzyka i zarządzania nim, a nie zaś stosowaniem metod *deriskingu* staje się również zrozumiałym wobec ryzyka związanego z procederem finansowania działań terrorystycznych. Styczność instytucji obowiązanej, zwłaszcza generalnego zaufania publicznego i zaufania wobec już obsługiwanych klientów, z tym procederem może znacznie nadwyrężyć jej status zaufania a także działać odstraszająco wobec nowych, potencjalnych klientów. Dotyczy to zwłaszcza tych podmiotów, które nie znajdują się jako podmioty wyznaczone na różnych listach sankcyjnych w związku z podejrzeniami o wspieranie terroryzmu. Należy jednak zdawać sobie sprawę z tego, że świadome wyprowadzenie klienta z formalno-finansowego obrotu, powoduje utratę informacji o nim. Utrudnia to znacznie uzyskiwanie śladów takiej działalności, jej rejestrowanie poprzez transakcje oraz ewentualne sterowanie zachowaniami sprawców. Ucieczka tych klientów, wobec których zastosowano *derisking*, nie dość, że uświadamia ich w posiadaniu przez instytucję potencjalnej wiedzy o ich przestępczych zamiarach, to również powoduje

[39] Raport EBA, ESMA, EIOPA, Joint Opinion, on the risks of money laundering and terrorist financing (*op. cit*.), s. 8.

ucieczkę w nieformalne kanały płatności, co znacznie utrudnia śledzenie poczynań przestępczych. Konsekwencją jest także brak możliwości zamrożenia środków a to ma swoje przełożenie na nadal nienaruszone posługiwanie się aktywami przez podmioty zapewniające finansowanie działań terrorystycznych. Taki stan rzeczy wskazuje na obraz sytuacji, w której instytucje nie chcą dopuścić do powstania zdarzenia, które zakwalifikują jako podejrzane i które wymusi na nich czynności informowania jednostki analityki finansowej na podstawie raportu SAR, STR, czy doprowadzenia do wstrzymania transakcji lub dokonania blokady środków (wartości majątkowych) na rachunku.

Proces *debankingu* wywołał szeroką dyskusję w niektórych krajach, między innymi dotyczy to Australii[40]. Mając na uwadze zauważone problemy przedstawiono szereg wytycznych dla instytucji obowiązanych. Ministerstwo Skarbu zaleciło również bankom stosowanie pięciu środków „mających na celu zwiększenie przejrzystości, spójności i uczciwości wobec klientów indywidualnych i małych firm w odniesieniu do wszystkich decyzji dotyczących *debankingu*". Te środki przejrzystości obejmują: udokumentowanie powodów usunięcia klienta z banku, przedstawienie klientom pozbawionym rachunku bankowego uzasadnienia banku, zapewnienie klientom pozbawionym rachunku bankowego dostępu do wewnętrznych procedur rozstrzygania sporów, dostarczenie powiadomienia z co najmniej 30-dniowym wyprzedzeniem przed zamknięciem istniejących podstawowych usług bankowych klienta oraz samooświadczenie o przestrzeganiu powyższych środków. Innym motywem stosowania *debankingu* jest słabość wobec własnych możliwości właściwej oceny ryzyka w instytucji obowiązanej oraz możliwa kara ze strony organów kontroli co do nierealizowania obowiązków wynikających z przepisów odnośnie do oceny ryzyka instytucjonalnego i indywidualnego. Powodem jest tu więc obawa wysokiej kary za nierealizowanie obowiązków wynikających z przepisów AML/CFT. W pełni charakterystycznym dla australijskiego rynku finansowego źródłem *debankingu* ustalono, iż jest problem dotyczący konkurencji. Zidentyfikowany on został przez australijską Komisję ds. Konkurencji i Konsumentów (ACCC), która wskazała, że międzynarodowym firmom transferów pieniężnych bardzo łatwo jest otwierać i utrzymywać rachunki w Europie, podczas gdy w Australii były one wielokrotnie usuwane z banku[41]. Przy okazji stwierdzono także, że działania mieszczące się w *debanking-u* były również wymierzone w giełdy kryptowalut.

[40] We wrześniu 2021 roku dyrektor generalny FinTech Australia poinformował komisję senacką (Senacka Komisja Specjalna ds. Technologii Finansowych), że około 150 członków tej organizacji zostało usuniętych z banku przez instytucje finansowe, bez podania przyczyny ani możliwości odwołania się od tej decyzji. W Chinach firmy zajmujące się kryptowalutami zostały niedawno zakazane i poddane *debanking*-owi z powodu decyzji politycznej dotyczącej kryptowaluty.

[41] De-banking questions, s. 1, (w:) file:///C:/Users/HP/Downloads/Fintech%20Australia%20-%20answer%20to%20QoNs.pdf.

W konsekwencji nieprzyznawania prawa do konta a tym samym prowadzenia szerszej obsługi przez nadzorowane instytucje finansowe powoduje, że zwłaszcza firmy związane z nowymi technologiami mogą sięgać po finansowanie *crowdfunding-owe*, bardziej niestabilne i mogące pochodzić z podejrzanych źródeł, niż sięganie po kredyty inwestycyjne instytucji finansowych, jako podmiotów obowiązanych. Dodatkową negatywną kwestią będzie to, że firmy mogą zdecydować się na prowadzenie działalności w zagranicznych jurysdykcjach, a ich zyski będą zwiększać dochód innych państw.

Należy zauważyć, że instytucje finansowe spotykają się aktualnie z różnego rodzaju ryzykami, które niekoniecznie należałoby łączyć z AML. Te specyficznie łączą się ze stosowaniem sankcji finansowych (i innych) wobec podmiotów, które wiązane są z terroryzmem i jego finansowanie. W konsekwencji wobec takich podmiotów wyznaczonych instytucje obowiązane zobligowane są do realizowania określonego rodzaju obowiązków, które stanowią tzw. szczególne środki ograniczające. Środki te polegają między innymi na nieudostępnieniu wartości majątkowych bezpośrednio ani pośrednio osobom i podmiotom, ani na ich rzecz, przez co rozumie się w szczególności nieudzielanie pożyczek, kredytu konsumenckiego lub kredytu hipotecznego, niedokonywanie darowizn, niedokonywanie płatności za towary lub usługi (art. 117 ust 2 pkt 2 ustawy o p.p.p.f.t.). Tym samym instytucja obowiązana we wskazanym zakresie nie wchodzi w relacje z podmiotem wyznaczonym. W tym przypadku nie ocenia się skali ryzyka a raczej reaguje wykonawczo na „zakaz prawny". Bazową sytuacją jest jednak dotychczasowe prowadzenie obsługi takich klientów. Niewiedza instytucji wobec niestwierdzenia powiązań z terroryzmem przed dokonaniem zamrożenia środków poszerza się też w przypadku niepodjęcia relacji z klientem. Jest to więc sytuacja podwójnego nierozpoznania ryzyka w instytucji obowiązanej, wiążącego klienta z aktywnością w zakresie finansowania terroryzmu.

We współczesnym świecie posiadanie konta bankowego stało się powszechnym i podstawowym elementem codziennego życia. To dość trywialne stwierdzenie stać się może w przypadku nie tyle niechęci, co niemożliwości posiadania konta dużym utrudnieniem. O ile ta trudność może dotyczyć relacji z pojedynczą instytucją finansową, to wydaje się, że ze względu na szeroki zakres usług finansowych i wielość instytucji nie sprawia to większej trudności. Zawsze możliwym jest skorzystanie z usług innej instytucji, która pozwoli na podpisane umowy o prowadzenie rachunku bankowego. Inaczej jest, gdy stosowane są platformy współpracy pomiędzy instytucjami finansowymi, na których prowadzi się między innymi wymianę informacji, o danych identyfikacyjnych osób/firm, którym odmówiono prowadzenia usług finansowych. Dotyczy to zwłaszcza kwestii prowadzenia rachunku bankowego. Taki stan rzeczy może prowadzić do stanu swoistej zmowy dyskryminacyjnej – nieobsługiwania klientów wywodzących się z określonego ustalonego rodzajowo sektora.

De-banking/de-risking versus the international AML/CFT system and special solutions for obligated institutions under Article 41 of the Act on Counteracting Money Laundering and Terrorist Financing (part 1)

Abstract

Practices referred to as de-banking *and* de-risking *should not be confused with anti-money laundering or terrorist financing procedures that are legally established and reasonably carried out. Generic non-provision of products and/or services by obligated institutions has no reasonable justification in terms of ensuring financial or economic security. Therefore, both* de-banking *and* de-risking *may contribute to higher risks and potential clients' leaving for the black and/or grey economy.*

Key words

De-banking, de-risking, AML/CFT, risk, identification, mitigants, financial security measures.