

Maciej Aleksander Kędzierski

Akademia im. L. Koźmińskiego w Warszawie

ORCID: 0000-0003-3074-1355

DERISKING/DEBANKING JAKO „METODY” ZAPEWNIANIA BEZPIECZEŃSTWA?

Wprowadzenie

Aktualne procedury przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (AML/CFT)¹ powinny być oparte na analizie ryzyka. Z czasem to wieloletnie już podejście wykazało także w niektórych przypadkach jego patologiczne wykorzystanie. Stąd też regulacje oparte na ocenie ryzyka skutkują dwoma typami instytucjonalnych negatywnych zachowań polegających na unikaniu ryzyka. Pierwszy sprowadza się do kreowania nadmiaru wewnętrznych polityk i procedur, w konsekwencji niezrozumiałych i niepolepszających jakości oceny ryzyka, drugi zaś związany jest z unikaniem obszarów wycenionych jako wiążące się z wysokim ryzykiem. Do tego drugiego typu zachowań zaliczymy *derisking* i *debanking*.

Derisking (wycofanie się z ryzyka)² stanowi indywidualne, zwłaszcza subiektywne, podejście do ryzyka reprezentowane przez określone instytucje zajmujące się na co dzień kwestiami świadczenia produktów i usług dla swoich klientów. Zachowanie to polega na całościowym, kompleksowym czy rodzajowym wykluczeniu możliwości obsługi określonych obszarów lub klientów zarówno na poziomie niepodpisywania umów o świadczenie produktów czy usług, jak i na poziomie wypowiedzania takim klientem już prowadzonych usług, zwłaszcza w zakresie obsługi finansowej czy prowadzenia konta bankowego (w tym przypadku ta specyficzna odmiana nieświadczenia lub odmowy świadczenia usług określana jest jako *debanking*, *debankowanie*).

¹ Skrótowiec ang. *Anti Money Laundering/Counter Financing of Terrorism* (przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu).

² *Derisk* – uczynić coś bezpieczniejszym, zmniejszając prawdopodobieństwo, że stanie się coś złego i że pieniądze zostaną utracone. <https://dictionary.cambridge.org/dictionary/english/derisk> (10.05.2024).

Obydwa rodzaje zachowań – *derisking* i *debanking* – można odnieść do postępowania instytucji obowiązanych (dalej: IO) w celu unikania regulacji lub niewłaściwego wykorzystania regulacji w zakresie przeciwdziałania przestępstwom (głównie związanych z AML/CFT, ale również z innych powodów, np. komercyjnych, politycznych), a także niedopuszczenia do konfrontacji z niepewnością, zwłaszcza cechowaną zagrożeniem oraz niedopuszczenia do podjęcia wysiłku zarządzania tego rodzaju ryzykiem poprzez niedoprowadzenie do wejścia w relacje IO–klient, z *a priori* przyjętym (założonym) określonym ryzykiem (niejednokrotnie niewycenionym indywidualnie w danej IO, a opartym na generalnych ocenach). Dlatego też IO zamiast zarządzać ryzykownymi klientami, decydują się na całkowite zakończenie relacji z nimi lub w ogóle nienawiązanie ich, co w konsekwencji minimalizuje ich własną ekspozycję na ryzyko, zwłaszcza gdy przewidują one, iż relacja z danym rodzajem klienta powodować będzie przekroczenie apetytu na ryzyko. Tym samym następuje negatywna segmentacja niedopuszczająca do sprzężeń zwrotnych w relacji rodzajowej. Powstaje więc tym samym sytuacja pozornego unikania ryzyka, a nie doprowadzenie do sytuacji zarządzania ryzykiem zgodnie z podejściem FATF (Grupa Zadaniowa ds. Przeciwdziałania Praniu Pieniędzy, ang. Financial Action Task Force) opartym na ryzyku.

Takie zachowanie najczęściej usprawiedliwiane jest obawami dotyczącymi ponoszenia znacznych kosztów utrzymania ryzyka lub też pełną niechęcią do inwestowania w stabilizowanie takiego ryzyka. Przedmiotowe odejście do ryzyka poprzez jego *ex ante* odrzucenie może też w obszarze AML/CFT wiązać się z coraz większym wachlarzem obowiązków, jakie zmieniające się przepisy narzucają na IO, zwłaszcza wobec klientów wysokiego ryzyka. *Debanking* może być również oceniony jako negatywny element uboczny wobec wprowadzenia w systemach AML/CFT sędowania odpowiedzialności za wykonywanie identyfikacji i oceny ryzyka na IO. Szczególnie dotyczy to obszaru identyfikacji ryzyka instytucjonalnego, któremu bliżej jest do wewnętrznych polityk bezpieczeństwa banku niż do potrzeby analizy sprawy ryzyka indywidualnego klienta czy transakcji. Tak więc ten specyficzny *derisking* może być także wynikiem obawy o rentowność, respektowania wymogów ostrożnościowych, narażeniem się na odpowiedzialność podmiotów odpowiedzialnych za obszar *compliance*, odzwierciedleniem sytuacji gospodarczej po światowym kryzysie finansowym czy utraty ryzyka reputacji instytucjonalnej (zwłaszcza jeżeli chodzi o podmioty zaufania publicznego oraz podmioty o wysokiej konkurencyjności). Należy mieć na uwadze to, że *derisking* traktowany niesłusznie jako sposób „pozbywanie się ryzyka” nie powoduje ostatecznie takiej zakładanej fałszywie sytuacji. Ryzyko występuje zawsze, zostaje ono jedynie przemieszczone do innych obszarów społeczno-finansowych, niekoniecznie podlegając umniejszeniu. Konsekwencje niedopuszczenia do otwarcia rachunku bankowego lub dokonania rozwiązania umowy są coraz bardziej dolegliwe, szczególnie gdy chodzi o ograniczanie obrotu gotówkowego albo wiązanie

tęgo zdarzenia z posiadaniem rachunku bankowego jako podstawowego kryterium do realizacji innego rodzaju usług, np. niebankowych (m.in. rozliczenia podatkowe, płatności internetowe, zarządzanie ubezpieczeniami).

Derisking to także niejednokrotnie reakcja IO na zdarzenia geopolityczne, stąd tego rodzaju rozwiązania dotyczą członków diaspory z takich państw, jak: Somalia, Rosja i Iran³. *Debanking* jest więc elementem obrony przed niechcianym klientem. Niestety, czasami staje się efektem wprowadzania jedynie częściowo lub na poziomie wymaganego ewidentnego minimum zaleceń FATF w obszarze AML/CFT. Może być również rezultatem swobody w zakresie tworzenia własnych polityk bezpieczeństwa, w tym oceniania możliwości utrzymania ryzyka AML/CFT, co może w przyszłości powodować konflikt między organami regulacyjnymi a nadzorowanymi przez nie IO. Przeciwwstawieniem się tego typu tendencjom może być wprowadzenie ogólnokrajowych rozwiązań prawnych znacząco obwarowujących warunkami rezygnację IO z obsługi rodzajowo określonego klienta lub też oceny stanu ryzyka ML/FT wycenione w krajowej ocenie ryzyka (KOR), za które ponosi odpowiedzialność państwowa jednostka analityki finansowej (w Polsce – Generalny Inspektor Informacji Finansowej, GIIF). Wobec powyższego już teraz można mówić o zjawisku mającym swoje ugruntowanie w tzw. rosnącym ryzyku debankingu (coś, co miało być eliminacją ryzyka, staje się jego źródłem).

Przedmiotem artykułu jest zaprezentowanie sposobu postępowania IO (decydentów władczych) przy użyciu „metody” *deriskingu/debankingu* w celu „pozbywania się” różnego rodzaju ryzyka, w tym ryzyka ML/FT, a w rzeczywistości dokonanie oceny takiego postępowania na podstawie przykładów działań w poszczególnych krajach. Ponadto zaprezentowano, czym jest *derisking* i jak może być on wykorzystany jako instrument przeciwdziałania ML/FT, ale także w realizacji służb państwowych jako element czynnej aktywności na rzecz „zapewniania bezpieczeństwa” w sytuacjach kryzysowych niezwiązanych z praniem pieniędzy oraz finansowaniem terroryzmu. Jako metodę zastosowano przegląd rozwiązań prawnych w poszczególnych krajach, w których *derisking* w różnej postaci stał się sposobem na regulację społeczną, w tym występowania zwłaszcza negatywnych zjawisk na tle rasowym, finansowym, religijnym czy oporu społecznego (jako metoda polityczna). Podstawowym założeniem artykułu jest to, że *deriskingu* nie można uznać za metodę neutralizującą rodzajowe zagrożenie w obszarze prania pieniędzy oraz finansowania terroryzmu, jest on natomiast nadużywany czy realizowany jako schemat postępowania podmiotu władczego w różnych

³ Np. każdego roku somalijscy migranci z całego świata wysyłają do Somalii około 1,3 mld USD. Z tego około 215 mln USD pochodzi ze Stanów Zjednoczonych (16%), co jest porównywalne z łączną kwotą pomocy rozwojowej i humanitarnej, jaką rząd USA wysłał do Somalii w 2012 r. (242 mln USD). Przekazy pieniężne utrzymują przy życiu 1 na 4 z 10 mln Somalijczyków mieszkających w tym kraju. *The Somali Remittance Crisis: when remittances are needed the most*, <https://crosstechpayments.com/somalian-remittance-crisis/> (20.04.2024).

sferach obrony przed innymi rodzajami zagrożeń bezpieczeństwa. Zachowania oparte na deriskingu/debankingu stają się przyczynkiem dla innego rodzaju zagrożeń, także tych, wobec których nie jest możliwe zastosowanie środków bezpieczeństwa finansowego.

Ocena przedmiotowego obszaru tematycznego

Główne czynniki, jakie brane są pod uwagę w zakres stosowania deriskingu, to: koszt, reputacja i potencjalne narażenie na przestępstwa finansowe. Do każdego z tych czynników IO powinna podchodzić synergicznie, nie forując jednych kosztów drugich, zwłaszcza dwóch pierwszych wobec trzeciego. Należy zauważyć, że system AML/CFT jest celowo ukierunkowany przede wszystkim na eliminację zagrożeń dla IO, szczególnie wobec narażenia jej na proceder przestępczy określony jako pranie pieniędzy czy finansowanie terroryzmu. Czynnikiem eliminującym przestępczość wydaje się być dominujący. Zwłaszcza *debanking* zwraca uwagę na istotną rolę banków w zarządzaniu finansami danego państwa, ale także na to, że same te instytucje, uzyskując wysoką pozycję w sprawach gospodarczych czy obsługi obywateli, nie chcą uczestniczyć w określonego rodzaju, co najmniej wątpliwych aktywnościach obywatelskich i podmiotów gospodarczych. Taka rola kreowana przez nie same powoduje wpływ na globalną ocenę stosunku różnego rodzaju instytucji, w tym państwowych, do określonych kategorii aktywności społecznych. Nie dotyczą one wyłącznie źródeł popełniania czynów zabronionych. Przykładem jest tu zastosowanie debankingu wobec zdecentralizowanych systemów finansów opartych na technologii *blockchain* (np. gdy chodzi o obrót walutami wirtualnymi).

Takie „metodyczne” podejście posiada wiele uwarunkowań, jak: niepełna wiedza o tej branży finansowej, upatrywana konkurencyjność, budowanie nowych walut wirtualnych jako przeciwwagi dla rozliczeń finansowych pomiędzy państwami objętymi sankcjami gospodarczymi, brak instrumentów i instytucji nadzorczych nad wykonawstwem, brak przepisów regulacyjnych, niemożność sprostania wymaganiom AML/CFT, a tym samym obawy przed nałożeniem kar, niedostawianie samego systemu AML/CFT do nowych rozwiązań finansowych (choćby wprowadzenia tego rodzaju instytucji do katalogu – IO). Co istotne jednak, mając na względzie to, że zdecentralizowane systemy finansów wkomponowały się już na trwałe w relacje gospodarcze, podmioty decyzyjne z czasem wprowadziły przepisy regulacyjne, włączając do obszaru AML/CFT również tego typu działalność (podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług obrotu walutami wirtualnymi)⁴. Tym samym zapobiegnięto stosowaniu na szeroką

⁴ Podobnie podmioty prowadzące system rozrachunku oparty na DLT, o którym mowa w art. 2 pkt 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/858 z 30 maja 2022 r. w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego

skalę debankingu wobec zdecentralizowanych systemów finansów. Ma to istotne znaczenie, ponieważ najważniejsze wydaje się zarządzanie ryzykiem. Tu działa ten schemat obosiecznie – z jednej strony ryzyko AML/CFT w ramach zdecentralizowanych systemów finansów nie jest do końca rozpoznawalne, a z drugiej strony sam ten system jest podatny na nieprawidłowości i zagrożenia ze strony sprawców, którzy chcą wykorzystać jego luki w zabezpieczeniach i oszukać użytkowników. Staje się więc „bezbronny” wobec uczciwych użytkowników. Nie sprzyja temu też postawa banków realizowana na zasadzie *deriskingu*, a więc oddalenia od siebie roli „ochronnej”, budowanej na zasadzie indywidualnej oceny ryzyka. Odrzucenie obsługi tego typu usług finansowych dla „trudnych” klientów jest naturalnym atutem antybankowym, który wobec „odrzuconych użytkowników” staje się kreatorem paralelnego rynku usług finansowych bez obowiązku oceny ryzyka tak jak w przypadku reprezentantów tradycyjnych usług bankowych.

Należy mieć na uwadze również to, że zwłaszcza *debanking* pozostaje w sprzeczności z pozyskiwaniem dowodów działalności przestępczej sprawców prania pieniędzy czy finansowania terroryzmu. To powoduje w pierwszym przypadku brak wiedzy o pierwotnych czynach zabronionych, a w drugim brak możliwości ustalenia beneficjenta terrorystycznego, którego można byłoby (potencjalnie) kojarzyć z organizacją zamachu terrorystycznego. Poprzez *debanking* przerywa się wiedzę instytucjonalną (w przypadku IO) oraz wiedzę operacyjną (w przypadku służb) i dowodową (w przypadku postępowań prokuratorskich i przed sądem) celem wykazania sprawczych powiązań i schematów sieciowych powiązań aktywów finansowych i rzeczowych pomiędzy sprawcami łańcucha dostaw dla terrorystów czy legalizacji aktywów uzyskanych w wyniku dokonania czynów zabronionych.

Ocena tych specyficznych zachowań instytucjonalnych związana była początkowo z niekoniecznie właściwie pojmowanym zakresem stosowania przepisów dotyczących AML/CFT. Podstawową zasadą w kontekście AML/CFT jest identyfikacja i ocena ryzyka instytucjonalnego i indywidualnego, zwłaszcza związanego z określonym klientem lub transakcją, czyli wzięcie oceny ryzyka „na siebie” przez IO, a dopiero w konsekwencji wystąpienia niemożliwości oceny ryzyka, pozostającego zwłaszcza po stronie klienta, odstępianie od podejmowania relacji gospodarczych czy zrealizowania transakcji okazjonalnej. Zalecenia FATF wymagają od instytucji finansowych zakończenia relacji z klientami jedynie w indywidualnych przypadkach, gdy nie można złagodzić ryzyka prania pieniędzy i finansowania terroryzmu. Nie jest jednak zgodne ze standardami FATF stosowanie hurtowego odcinania całych klas klientów bez poważnego i kompleksowego uwzględnienia ich poziomu ryzyka lub środków ograniczających ryzyko

rejestr, a także zmiany rozporządzeń (UE) nr 600/2014 i (UE) nr 909/2014 oraz dyrektywy 2014/65/UE (Dz.Urz. UE L 151 z 2.06.2022, s. 1).

dla poszczególnych klientów w ramach określonego sektora⁵. Podejście to zakłada więc indywidualną i specyficzną dla danej IO ocenę ryzyka. Natomiast w konsekwencji walki z finansowaniem terroryzmu i samym terroryzmem wprowadzono dodatkowo instrument zamrażania środków finansowych, jakimi dysponują podmioty wyznaczone na listach sankcyjnych (ONZ, Unii Europejskiej, poszczególnych krajów). Ta formuła przeciwdziałania także zawierała w swoim założeniu podejście indywidualne, lecz z czasem zaczęła dotyczyć nie tylko poszczególnych podmiotów, ale też państw (np. Iran, Syria) postrzeganych jako podmioty prawa międzynarodowego wspierające działalność terrorystyczną. W rezultacie zastosowanie deriskingu uniemożliwia:

- monitoring klienta/transakcji, a tym samym pozyskiwanie wiedzy na temat możliwych i ewentualnych powiązań z procederem prania pieniędzy oraz finansowania terroryzmu,
- identyfikowanie źródeł pochodzenia i sposobów przemieszczania środków do/ z systemu ich legalizacji lub beneficjentów terrorystycznych,
- prawidłowe stosowanie mechanizmów systemu AML/CFT, ponieważ klienci niebędący w relacji z IO nie będą przekazywać wszystkich informacji, a zwłaszcza tych, które by ich eliminowały z utrzymywania w dalszym czasie relacji gospodarczych z IO (nie powoduje to także sytuacji wzajemnego zaufania),
- współdziałanie ze sobą kilku tożsamyh rodzajowo lub różnorodnych rodzajowo IO na rzecz wspólnego monitorowania zachowań klienta podejrzewanego o powiązania z procederem prania pieniędzy lub finansowania terroryzmu,
- identyfikowanie aktywów w celu ich zamrażania (stosowanie szczególnych środków ograniczających) lub wstrzymania dystrybucji (blokady konta, wstrzymania transakcji podejrzanej),
- realizowanie właściwej współpracy w zakresie wymiany informacji pomiędzy jednostkami wywiadu finansowego (jednostki nie są zasilane informacją rozpoznania i jej transpozycji na informację finansową),
- przeciwstawienie się budowaniu alternatywnych kanałów przepływu aktywów, które nie kontrolują ryzyka, a wręcz bazują na jego nierozpoznawalności, tym samym stając się anonimowym instrumentem sprzyjającym na rzecz popełniania przestępstw,
- dokonanie oceny, jak dany produkt/usługa IO będzie postrzegana wobec danej rodzajowo zbiorowości, czyli na ile będzie niewłaściwie wykorzystana, a na ile będzie ona inicjowała działania do popełniania przestępstw,
- zbudowanie zbioru uczącego, gdy IO będzie chciała skorzystać z zasilenia procedury rozpoznania ryzyka za pomocą sztucznej inteligencji.

Debanking wymierzony w członków Al-Kaidy, jako członków organizacji terrorystycznej, przekształcił się w podstawowe narzędzie używane przeciwko „krajom

⁵ *De-risking, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism*, <https://www.coe.int/en/web/moneyval/implementation/de-risking> (2.05.2024).

zbójcekim”, takim jak Iran i Korea Północna. Również innego rodzaju sankcje, ale też opierające się na schemacie zamrażania środków, dotyczą państw, które naruszały prawa człowieka lub wzniecały konflikty zbrojne (np. Białoruś, Rosja). Zamykanie rachunków bankowych i nierealizowanie międzynarodowych przekazów pieniężnych posiada swoje odzwierciedlenie w restrykcyjnych działaniach wymierzonych przynajmniej w dwóch kierunkach. Pierwszy związany jest z nieszanowaniem rachunków instytucji pośrednictwa finansowego dokonujących przesyłu środków z państw Unii Europejskiej do państw zwłaszcza afrykańskich, w których nie obowiązują europejskie standardy w zakresie rozliczeń finansowych. Związane jest to przede wszystkim z tym, że obrót realizowany jest poprzez przekazy internetowe, gdzie obrót gotówkowy jest minimalny, ponieważ jest związany z tym, że posiadanie gotówki narażone jest na zagrożenia związane z wysokim stopniem przestępczości pospolitej. Tym samym osoby migrujące do Unii Europejskiej i chcące utrzymywać relacje finansowe z krajem pochodzenia nie mają takich możliwości w zakresie wykorzystania do tego nadzorowanych IO o charakterze finansowym. Drugi kierunek jest podobny, ale związany z pochodzeniem migrantów z krajów objętych sankcjami m.in. w związku ze społecznym, ale głównie przez organy władzy wykonawczej popieraniem działań terrorystycznych, ich finansowaniem czy też wspieraniem konfliktów zbrojnych. Przyszłościowo drugi kierunek może zostać poszerzony o niektóre państwa afrykańskie (Mali, Burkina Faso, Niger) w związku z realizacją umów finansowo-militarnych z Federacją Rosyjską. W konsekwencji banki zamykają rachunki MSB (to nierejestrowane w jednostce analityki finansowej podmioty świadczące działalność w zakresie usług płatniczych, *money services businesses*) i międzynarodowych przekazów pieniężnych, które zapewniają utrzymanie powiązań finansowych między diasporami relokowanymi w danym kraju (np. Unia Europejska, Kanada) a ich przyjaciółmi/akolitami, rodzinami i małymi firmami w ich bardziej ryzykownych krajach pochodzenia⁶. Ponadto rugowanie takich podmiotów jak MSB związane jest z posiadaniem przez nie nieadekwatnych pod względem zabezpieczeń systemów ochrony, jakimi dysponują duże bankowe przedsiębiorstwa. W konsekwencji negatywna postawa wobec tego rodzaju podmiotów może zmusić je do podjęcia działalności w czarnej lub szarej strefie gospodarczej (nie mogą one konkurować z wysokospecjalistycznymi instytucjami jak banki). Tym samym *debanking* nie wyeliminuje ryzyka związanego z transakcyjnością i nie doprowadzi do możliwości pozyskiwania „śladów transakcyjnych” podejrzanych przepływów środków finansowych docelowo legalizowanych lub przeznaczanych dla beneficjentów terrorystycznych. Innym sposobem usprawiedliwienia debankingu jest powoływanie się na rejestry skazanych. Umieszczenie klienta w rejestrze karnym może stanowić przeszkodę w dostępie do podstawowych usług, takich

⁶ Zob. M. Lemieux, *De-banking international money remitters in Canada*, 2018, <https://www.linkedin.com/pulse/de-banking-international-money-remitters-canada-marc-lemieux> (14.05.2024).

jak konto bankowe. Banki i ubezpieczyciele mogą więc szerzej również dyskryminować osoby z niezatartymi wyrokami skazującymi, firmy Fintech czy firmy rynku Forex.

Polskie rozwiązania prawne w zakresie deriskingu znajdują się w art. 41 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu⁷. Może być on rozumiany jako *derisking*, gdy dotyczy wszystkich rodzajów IO, a w przypadku, gdy mamy do czynienia z bankiem jako IO, można określić go mianem *debankingu*. Zarówno *derisking*, jak i *debanking* w systemie AML/CFT, gdy nie posiada umocowania prawnego i umotywowania w ściśle określonych przepisach rangi ustawy, należałoby ocenić pejoratywnie. System AML/CFT, mimo że dotyczy dwóch kwestii podstawowych, tj. przeciwstawienia się procederowi prania pieniędzy oraz finansowania terroryzmu, to jednak dotyka szeregu innych obszarów bezpieczeństwa: przestępstw pierwotnych (źródłowych) jako czynów zabronionych dla przestępstwa z art. 299 k.k., samego zjawiska terroryzmu, relacji negatywnych pomiędzy terroryzmem a przestępczością zorganizowaną, pośrednio także przestępczości podatkowej, finansowej, działania na szkodę podmiotów zaufania publicznego, korupcji, proliferacji broni masowego rażenia oraz materiałów podwójnego wykorzystania. Należy ponadto zaznaczyć, że zapis art. 41 u.p.p.p.f.t. w ust. 1 wprost wskazuje, że niedopuszczenie do relacji z klientem lub rozwiązanie w tym zakresie stosunków gospodarczych związane jest z niemożliwością zastosowania jednego ze środków bezpieczeństwa finansowego, o którym mowa w art. 34 ust. 1 u.p.p.p.f.t., a więc opiera się na rozstrzygnięciu indywidualnym, a nie działaniu wymierzonym w rodzajowo określonych klientów. Taki kierunek także pozostaje słuszny wobec wytycznych określanych przez FATF⁸. Omawiana ustawa wskazuje też, że wobec podmiotów wyznaczonych na listach sankcyjnych podejmuje się szczególne środki ograniczające. Polegają one m.in. 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 u.p.p.p.f.t.). Jest to więc działanie, które także będzie można zaliczyć do debankingu (*deriskingu*), ale skierowanego wobec indywidualnych podmiotów, a nie całych ich zbiorowości.

W konsekwencji zaprezentowanych przepisów można wyróżnić te, które odnoszą się do AML/CFT, oraz te, które na gruncie prawa krajowego na wzór i podobnie regulują kwestie zamrażania środków i reagowania na innego rodzaju sankcji niż te związane z praniem pieniędzy, a zwłaszcza przeciwdziałaniem finansowaniu

⁷ Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2023, poz. 1124, 1285, 1723, 1843), dalej: u.p.p.p.f.t.

⁸ The Financial Action Task Force (FATF), Grupa Zadaniowa ds. Przeciwdziałania Praniu Pieniędzy.

terroryzmu. W polskich warunkach prawnych do tych przepisów będzie można zaliczyć przepisy regulujące kwestię przeciwdziałania przestępczości podatkowej i system STIR⁹ (Dział 3B – Przeciwdziałanie wykorzystywaniu sektora finansowego do wyłudzeń skarbowych – Ordynacja podatkowa) oraz przepisy dotyczące przeciwdziałania związanego ze szczególnymi sankcjami (środkami ograniczającymi) nałożonymi na podmioty rosyjskie w związku z inwazją na Ukrainę w 2022 r.¹⁰ Inną konsekwencją wprowadzanych przepisów jest zastosowanie na poziomie IO wzmocnienia środków bezpieczeństwa finansowego a w szczególności identyfikacji i weryfikacji klienta (*Know Your Client* – KYC, poznaj swojego klienta; *Know Your Transaction* – KYT, poznaj swoją transakcję), tak aby nie być narażonym na zarzut uniknięcia ryzyka obchodzenia sankcji, także poprzez *derisking* i *debanking*. Co zastanawiające, tego typu rozwiązania, stworzone zwłaszcza w celu przeciwdziałania zagrożeniu związanemu z przestępczymi procederami ML/FT, ustanowione zostały również na rzecz innych działań związanych z zapewnieniem bezpieczeństwa. Tym samym rodzajowo wykonywany *derisking* IO pozostaje w sprzeczności z misją realizowaną w ramach partnerstwa publiczno-prywatnego, aby to także wskazane ustawowo IO uczestniczyły w szeroko rozumianym systemie przeciwdziałania przestępczości. To samo stwierdzenie odnosi się do innych systemów niż AML/CFT, ale zintegrowanych z nim na potrzeby rozpoznawania innych kategorii zagrożeń.

Należy zauważyć, że stosowanie *deriskingu* i *debankingu* może być związane nie tylko z ustaleniem indywidualnej sytuacji uprawniającej do takiego postępowania przez IO. Może być również rezultatem dokonania oceny ryzyka instytucjonalnego czy prowadzenia wewnętrznej polityki bezpieczeństwa w takiej instytucji, a w konsekwencji odrzucenia określonych kategorii klientów. Może więc wynikać z pierwotnie określonego zawężenia pola bezpieczeństwa IO czy wytypowania kategorii negatywnych (zagrożeniowych). Kwestie te miały miejsce m.in. wobec nienadzorowanych instytucji pośrednictwa finansowego czy podmiotów zajmujących się obrotem walutami wirtualnymi. Te kategorie wyalienowania były prawdopodobnie związane z odrzuceniem związanym z niewiedzą, nieprzygotowaniem, a zwłaszcza z niemożliwością racjonalnej oceny skali ryzyka przez pracowników instytucji w związku z ryzykiem, jakie te podmioty ze sobą niosły. Zatem związane z odrzuceniem działalności w sytuacji niepewności wobec innych sytuacji niż ML/FT, pozwalających na ocenę prawdopodobieństwa i skali określonego ryzyka.

⁹ Przepisy o systemie teleinformatycznym izby rozliczeniowej zwanym STIR obowiązują od stycznia 2018 r. (w pełnym, sankcyjnym zakresie – od kwietnia 2018 r.) i mają na celu przeciwdziałanie wykorzystywaniu sektora finansowego do wyłudzeń skarbowych.

¹⁰ Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. 2023, poz. 129, 185).

Amerykańskie próby regulacji debankingu na tle dyskryminacji rasowej, religijnej i narodowej

Historia debankingu w Stanach Zjednoczonych posiada swoje początki w latach 2000. XX w. Około 2005 r. banki w USA zaczęły zamykać konta operatorów przekazów pieniężnych, głównie małych firm etnicznych. Działania te były związane z aktywnością ekonomiczną, zwłaszcza diaspory pochodzenia latynoskiego, i dokonywaniem przekazów pieniężnych do kraju urodzenia celem wsparcia ekonomicznego rodzin. Kwoty przekazów były niewielkie, ale ich liczba była bardzo wysoka, co miało swoje odzwierciedlenie w wypływie kapitału poza kraj. Pojawiły się także, oceny według których to właśnie emigranci latynoscy prali pieniądze na wielką skalę. W 2010 r. Kongres Stanów Zjednoczonych uchwalił, a prezydent podpisał Dodd-Frank Wall Street Reform and Consumer Protection Act¹¹. Ustawa ta była początkiem przeciwdziałania deriskingowi i debankingowi ze względu na odmienność rasy i koloru skóry. Na jej podstawie utworzono Biuro Ochrony Finansowej Konsumentów (Consumer Financial Protection Bureau – CFPB), którego zadaniem była ochrona konsumentów-klientów IO przed takimi praktykami¹².

Niestety pojedyncze przypadki odmawiania usług bankowych przerodziły się w trend rynkowy. W szczególności duże banki zaczęły wykorzystywać swoją rolę na rynku usług finansowych, a jednocześnie kształtować własną, im sprzyjającą „politykę bezpieczeństwa”. W 2019 r. JP Morgan Chase przestał świadczyć usługi dla prywatnych więźniów po protestach, które odbyły się przed domem prezesa J. Dimona. Bank twierdził, że jego działanie było wynikiem oceny „kosztów i korzyści” obsługi branży. Kilka banków i firm przetwarzających płatności, w tym PayPal, Citibank i Bank of America, zerwało więzi z producentami broni i powiązаныmi firmami. Bank of America dołączył do pięciu innych dużych amerykańskich banków, aby stanąć na stanowisku, że nie będzie finansował żadnych działań związanych z ropą i gazem w Arctic National Wildlife Refuge, mimo że rząd federalny stworzył go na rzecz poszukiwania i produkcji. Bank określił swoją

¹¹ U.S. Congress, H.R.4173, *Dodd-Frank Wall Street Reform and Consumer Protection Act*, <https://www.congress.gov/bill/111th-congress/house-bill/4173/text> (16.05.2024).

¹² Przykładem jest tu odmawianie wydawania kart kredytowych osobom narodowości ormiańskiej przez Citi Bank (kara w wysokości 25,9 mln USD grzywny i zadośćuczynienie konsumentom za zamierzone i nielegalne dyskryminowanie osób ubiegających się o karty kredytowe w latach 2015–2021). Organy nadzoru Citi kamuflowały wewnętrzne procedury, aby ukryć praktyki dyskryminacyjne, instruując pracowników, aby nie omawiali z potencjalnym klientem dyskryminacyjnych praktyk poprzez utrwalanie ich pisemnie lub poprzez nagrywanie na linii telefonicznej. Pracownicy Citi kłamali także na temat podstaw odmowy, podając fałszywe powody kandydatom ubiegającym się o wydanie kart kredytowych. Selekcji negatywnej klientów dokonywano poprzez analizę zapisów nazwisk. Consumer Financial Protection Bureau’s Post, https://www.linkedin.com/posts/consumer-financial-protection-bureau_cfpb-orders-citi-to-pay-259-million-for-activity-7128032053530357763-8oX1 (16.05.2024).

decyzję jako kodyfikację istniejącej praktyki¹³. Banki nie tylko postanowiły zaprzestać udzielania pożyczek na niektóre projekty poszukiwawcze i produkcyjne w Arktyce, ale także zaprzestały świadczenia usług finansowych niezwiązanych z ryzykiem kredytowym lub operacyjnym dla niektórych gałęzi przemysłu energetycznego, w tym wydobywania węgla w całym regionie Arktyki.

Banki często uzasadniają odmowę świadczenia usług określonym kategoriom przedsiębiorstw, opierając się na postrzeganiu ryzyka utraty reputacji, a nie na indywidualnym określeniu ryzyka związanego z każdym klientem¹⁴. W konsekwencji debankingu staje się elementem szerszej polityki podmiotów prywatnych, który może przerodzić się w przyszłości w niebezpieczny instrument prowadzenia tej polityki równoległe (lub jako jej element) do polityki reprezentowanej przez władzę państwową. Oznacza to, że może się on stać nie tyle instrumentem bezpieczeństwa, co instrumentem pobudzającym innego rodzaju zagrożenia, z którymi należałoby walczyć na zasadzie identyfikacji i oceny pod kątem kreowanego ryzyka, nie zaś wypierania go poza obszar obsługi finansowej. Ponadto, co bardziej niebezpieczne, dla usankcjonowania takiego postępowania kreuje się także sposób powoływania na niedookreślone pojęcia, np. na „ryzyko reputacji”. *De-banking* może być elementem niewiedzy o zagrożeniu, z czego mogą korzystać inne instytucje, przyjmując wyrugowane podmioty pod swoją obsługę, niekoniecznie jednak mogą to być podmioty prywatne, ale również podmioty kontrolowane przez poszczególne państwa lub podmioty z pełnym kapitałem państwowym. W konsekwencji tego rodzaju aktywność może stać się elementem „nowej wojny” w sferze pójsicia na skróty, opieki „pokrzywdzonych”, a cel – odrzucony przez inne podmioty chociażby ze względu na prestiż lub grupy nacisku – może być elementem uzyskania przewagi nad określonymi ważnymi militarnie i gospodarczo obszarami (np. jako element wojny hybrydowej lub kognitywnej). Zwłaszcza w obszarze „wojny kognitywnej” podatne mogą być tu, w wyniku stosowania debankingu, grupy osób rodzajowo odrzucone w zakresie obsługi finansowej (np. poprzez powszechne dyskredytowanie roli banków jako filarów finansowych państwa), ale też pozasystemowe i pozabankowe instytucje finansowe mogą być instrumentem sabotażu finansowego i pozyskiwania źródeł informacji przez służby zagraniczne (np. na podstawie udzielania korzystnych indywidualnych pożyczek gotówkowych). Tym samym niezbędne staje się przyjęcie rozwiązań zapobiegającym debankingowi w skali, w jakiej ten negatywny trend może zagrozić bezpieczeństwu państwa. Amerykańskie Biuro Kontrolera Waluty (The Office of the Comptroller of the Currency – OCC) ogłosiło przepis (zasadę), który skutecznie uniemożliwiłby największym bankom w kraju odmawianie usług spółkom w dobrej kondycji z powodów reputacyjnych. Zasada

¹³ E.R. Wald, *Debanking Hurts Everyone*, 2021, <https://www.barrons.com/articles/debanking-hurts-everyone-51610145010> (10.05.2024).

¹⁴ *Ibidem*.

ta, zwana powszechnie „zasadą sprawiedliwego dostępu” (Fair Access to Financial Services), została wydana 14 stycznia 2021 r. i miała wejść w życie 1 kwietnia 2021 r. Decyzja o jej skutecznieniu została jednak odroczonej w czasie. Zgodnie z zasadą sprawiedliwego dostępu banki objęte nią byłyby zobowiązane w następującym zakresie:

- usługi finansowe, które bank zdecyduje się zaoferować w obszarach geograficznych, w których działa, byłyby dostępne dla wszystkich klientów w oparciu o ilościowe, bezstronne standardy banku oparte na ryzyku, a nie w oparciu o to, czy klient należy do określonej kategorii klientów,
- banki oceniałyby ryzyko stwarzane przez poszczególnych klientów na zasadzie indywidualnej, a nie w oparciu o ocenę kategorii,
- banki wdrażałyby kontrole w celu zarządzania relacjami współmiernie do tych ryzyka związanego z każdym klientem, a nie wprowadzałyby strategii całkowitego unikania poszczególnych branż lub kategorii klientów¹⁵.

Banki mają swobodę świadczenia lub odmowy świadczenia usług finansowych każdemu indywidualnemu klientowi, ale najpierw muszą oprzeć się na danych empirycznych, które są oceniane zgodnie z ustalonymi, bezstronnymi standardami zarządzania ryzykiem obowiązującymi w banku. Kolejno w lipcu 2022 r. grupa senatorów demokratycznych ponownie wprowadziła do trybu legislacyjnego ustawę o sprawiedliwym dostępie do usług finansowych, która zabrania bankom dyskryminacji ze względu na rasę, kolor skóry, religię, narodowość, płeć, orientację seksualną lub tożsamość seksualną. Projekt ustawy zapewniłby wszystkim konsumentom równe traktowanie w dostępie do towarów i usług w instytucjach finansowych¹⁶. Ustawa o sprawiedliwym dostępie do usług finansowych miała na celu zapewnienie równego traktowania wszystkich osób próbujących uzyskać dostęp do usług instytucji finansowych. Pociągnęłaby również instytucje do odpowiedzialności za praktyki dyskryminacyjne. W nowej propozycji wskazano, że wszystkie osoby mają prawo do pełnego i równego korzystania z towarów, usług, urządzeń, przywilejów i udogodnień każdej instytucji finansowej zgodnie z definicją zawartą w sekcji 803 ustawy o nadzorze nad płatnościami, rozliczeniami i rozrachunkami z 2010 r. (12 U.S.C. 5462), bez dyskryminacji ze względu na rasę, kolor skóry, religię, pochodzenie narodowe i płeć (w tym orientację seksualną i tożsamość płciową). W każdym przypadku, gdy jakakolwiek osoba podjęła lub istnieją uzasadnione powody, aby sądzić, że jakakolwiek osoba ma

¹⁵ S.563 sekcja 2 pkt 10 ppkt A–C – Fair Access to Banking Act, <https://www.congress.gov/bill/117th-congress/senate-bill/563/text> (10.05.2024); A.P. Price, S.M. Dollar, *Newly promulgated “Fair Access Rule” could alter banks’ decision-making, but its future is uncertain*, <https://www.nortonrosefulbright.com/en-us/knowledge/publications/c41ff38e/newly-promulgated-fair-access-rule> (10.05.2024).

¹⁶ Ustawa o prawach obywatelskich z 1964 r. zakazała dyskryminacji wielu instytucji publicznych, nie obejmowała ona jednak instytucji finansowych.

zamiar podjąć działanie lub praktykę zabronioną wskazaną powyżej, osoba poszkodowana może wytoczyć powództwo cywilne o pomoc zapobiegawczą, w tym wniosek o wydanie stałego lub tymczasowego nakazu zaprzestania szkodliwych praktyk, nakazu powstrzymania się od działań lub innego nakazu.

Budowane aktualnie oraz funkcjonujące współcześnie struktury społeczne w większej mierze oparte są na korzystaniu z rachunku bankowego bądź też zawierają w swoich modelach wykonawczych potrzebę oparcia części rozwiązań na rachunku bankowym. Tym samym dolegliwość uniemożliwienia lub też wypowiedzenia umowy o prowadzenie rachunku bankowego staje się tak uciążliwa dla osób fizycznych i prawnych. Rozwój sfery obrotu bezgotówkowego, rozliczenia pomiędzy kontrahentami, e-urzędy, e-rozliczenia podatkowe, e-płatności, posługiwanie się kartami płatniczymi stale związane są z potrzebą posiadania konta bankowego. Ekonomiczne konsekwencje debankingu są ważne same w sobie, ponieważ nie można rozpocząć działalności gospodarczej, prowadzić organizacji *non-profit* lub uzyskać karty kredytowej czy kredytu hipotecznego bez konta bankowego. Nie można uzyskać także dostępu do systemu płatności, aby płacić rachunki lub wypisywać чеки, bez posiadania konta bankowego¹⁷.

Należałoby również przywołać prace i argumentację nad wprowadzeniem przepisów The Secure and Fair Enforcement Regulation Banking Act (SAFER Banking Act). To przykład propozycji uregulowania dostępu do usług bankowych dla firm zajmujących się dystrybucją produktów wytworzonych z marihuany, uznając wcześniej, że ten rodzaj działalności objęty jest „wykluczeniem finansowym”. W ciągu ostatniej dekady zalegalizowano w czterdziestu siedmiu stanach, czterech terytoriach USA i Dystrykcie Kolumbii jakąś formę marihuany medycznej lub rekreacyjnej – pomimo jej klasyfikacji jako nielegalnego narkotyku zgodnie z artykułem ustawy o substancjach kontrolowanych (21 USC § 801 i n.)¹⁸. Wskazano, że dotychczas ze względu na konflikt między prawem federalnym i stanowym wiele instytucji finansowych pozostaje niechętnych prowadzeniu interesów z legalnymi podmiotami objętymi sankcjami państwa. W rezultacie te firmy i ich pracownicy są zablokowani w dostępie do rachunków depozytowych, linii kredytowych i innych usług finansowych, w tym kredytów hipotecznych na cele komercyjne i mieszkaniowe, oraz akceptowaniu kart kredytowych i debetowych podczas prowadzenia działalności detalicznej. Wskazana regulacja SAFER miała temu zaradzić. Projekt ustawy, który wielokrotnie osiągał poziom umieszczenia go pod obrady w Izbie Reprezentantów, nie został wprowadzony w życie pomimo wielości prób jego ostatecznego uchwalenia. Jest to przykład, jak rozwiązania o charakterze debankingu podlegają rewitalizacji ze względu na określone

¹⁷ Zob. T. Zywicki, *Restoring the Rule of Law in Finance*, „FIRST PRINCIPLES” 2023, no. 92, <https://www.heritage.org/sites/default/files/2023-06/FP92.pdf> (17.05.2024).

¹⁸ SAFER Banking Act, https://www.democrats.senate.gov/imo/media/doc/safer_section_by_section.pdf (16.05.2024).

grupy nacisku polityczno-finansowego. Wolność rynkowa w tak specyficznym obszarze stawiana jest na równi z innymi przyczynami nierówności finansowych powiązanych z humanitarnymi prawami człowieka. Tak więc praktyki debankingu także wpływają na wolność jednostki (depersonalizacja), a nie tylko na ekonomię (deekonomizacja).

Brytyjskie doświadczenia w zakresie stosowania debankingu i jego przeciwdziałaniu

Raport Ogólnopartyjnej Grupy Parlamentarna ds. Uczciwej Bankowości Biznesowej (All Party Parliamentary Group on Fair Business Banking – APPG) opublikowany za 2023 r. wskazuje, że wspólną cechą łączącą grupy podlegające debankingowi jest postrzegany przez IO ich profil ryzyka odbiegający od normy¹⁹. Podane przykłady obejmują firmy zajmujące się kryptowalutami, polityków, jubilerów i brokerów jachtowych, którzy z różnych powodów są postrzegani jako problematyczni dla banków. W raporcie APPG wskazano, że banki mają obowiązek zwalczania przestępczości finansowej i muszą „nadzorować swoją bazę klientów, zarówno obecnych, jak i potencjalnych”, ponieważ stanowią oni pierwszą linię obrony przed osobami piorącymi pieniądze, terrorystami oraz innymi krajowymi i międzynarodowymi przestępcami. Stwierdzono, że głównym powodem, dla którego banki blokują klientom dostęp do swoich systemów finansowych, są koszty i reputacja, a nie zwalczanie przestępczości finansowej. Podobne do amerykańskich rozwiązania zostały wdrożone także w Wielkiej Brytanii. W 2023 r. Coutts, prywatny bank należący do Nat-Westa, ze względu na swoje poglądy rozwiązał umowę z byłym liderem UKIP i Partii Brexit, N. Farage’em. APPG również wskazała w raporcie, że zamykano konta „wszystkim grupom chrześcijańskim o kontrowersyjnych poglądach na temat homoseksualizmu i prawicowym blogerom, a także organizacjom związanym z branżą strzelecką”. Należy zauważyć, że art. 18 Regulaminu Rachunków Płatniczych zabrania tzw. debankingu osób ze względu na ich poglądy polityczne. H. Stephenson (dyrektor naczelny Komisji ds. Organizacji Dobroczynnych/Charytatywnych) stwierdził, iż potwierdzono, że w 2023 r. 42% z 2500 organizacji charytatywnych ankietowanych przez Komisję ds. Organizacji Charytatywnych miało problemy bankowe, w tym 6% doświadczyło nieoczekiwanego zamrożenia kont, a 7% potwierdziło, że ich banki utraciły dane. Jednocześnie zasugerowano, że brytyjskie banki mogą błędnie oznaczać konta klientów jako stwarzające ryzyko oszustwa, aby ukryć obawy dotyczące kosztów i swojej reputacji (błędna

¹⁹ <https://www.appgbanking.org.uk/articles-and-reports/> (2.05.2024). Obrazowo stwierdzono, że *debanking* jest „tęym narzędziem, które często nie jest ani skuteczne, ani sprawiedliwe”.

kategoryzacja)²⁰. Aby zapewnić klientom większą ochronę, Ministerstwo Skarbu zamierzało jak najszybciej zmienić przepisy (rozporządzenia 51 PSR 2017)²¹, nakładając na banki obowiązek:

- zapewnienia klientowi prawa do jasnego i stosowanego wyjaśnienia w przypadku, gdy jego konto zostało zamknięte, z wyjątkiem sytuacji, gdy byłoby to niezgodne z prawem,
- przy zamykaniu konta bank będzie musiał o tej decyzji powiadomić klienta z co najmniej 90-dniowym wyprzedzeniem, chyba że ma to miejsce w przypadku poważnego i nienaprawionego naruszenia, takiego jak brak płatności lub inne poważne zdarzenie; krótsze okresy wypowiedzenia będą dozwolone w pewnych okolicznościach, np. gdy dostawca usług płatniczych jest zobowiązany do rozwiązania umowy w celu wywiązania się z obowiązków wynikających z przestępstwa finansowego; będzie także możliwość zakwestionowanie decyzji przez klienta za pośrednictwem Rzecznika Finansowego lub znalezienie banku zastępczego.

Ponadto we wrześniu 2023 r. FCA (The Financial Conduct Authority, Urząd ds. Usług Finansowych) rozpoczął przegląd działań, w jaki sposób banki podejmują decyzje dotyczące otwierania lub zamykania rachunków prowadzonych dla PEP (Politically Exposed Persons), czyli „osoby zajmujące eksponowane stanowiska polityczne” (tzw. debanking polityków). Jednak w okolicznościach, w których ryzyko dla banków prowadzących rachunki operacyjne (w szczególności biorąc pod uwagę wzrost liczby osób objętych sankcjami) pozostaje poważne, wydaje się nieuniknione, że *debanking* będzie w dalszym ciągu wykorzystywany jako narzędzie zarządzania tym ryzykiem²².

Kanadyjskie rozwiązania prawne uwzględniające *derisking/debanking* wobec zagrożenia bezpieczeństwa

Do zaprezentowania pozostaje także kwestia związana z możliwością stosowania *deriskingu* i *debankingu* na polecenie władz krajowych w związku z potrzebą zapewnienia bezpieczeństwa publicznego. O ile bowiem wskazane powyżej przykłady związane są ze stosowaniem *debankingu* i *deriskingu* w imieniu

²⁰ Z danych FCA wynika, że w latach 2022–2023 z powodu przestępstw finansowych zamknięto około 185 000 rachunków, w porównaniu z około 72 000 w latach 2017–2018.

²¹ The Payment Services Regulations 2017, UK Statutory Instruments 2017 No. 752 PART 6 Framework contracts Regulation 51 [w:] The Payment Services Regulations 2017 UK Statutory Instruments 2017 No. 752 PART 6 Framework contracts Regulation 51, legislation.gov.uk (2.05.2024).

²² *De-banking – the potential pitfalls*, England and Wales 11.03.2024, <https://cms-lawnow.com/en/ealerts/2024/03/de-banking-the-potential-pitfalls> (2.05.2024).

i na rzecz podmiotów „prywatnych”, zwłaszcza mających status IO, to w tym zakresie te właśnie podmioty miałyby wykonywać polecenia wykonawczych władz centralnych w obszarze uniemożliwiania wchodzenia w relacje z określonymi rodzajami osób lub też masowo miałyby wypowiadać umowy o świadczenie produktów i usług już istniejącym klientom mającym negatywny status określony i nakazany przez władze państwową jako podmiot zewnętrzny. Tego typu rozwiązania nastąpiły w Kanadzie w związku z protestami ruchów antyszczepionkowych wobec szczepień na COVID-19. Protesty te przybrały one masowy charakter i powodowały blokadę stolicy kraju przez konwoje ciężarówek. Co istotne, wydaje się, że pojęcie deriskingu i debankingu należałoby traktować jako działanie poza systemem AML/CFT, jednak jest to stwierdzenie nieoczywiste, ponieważ to właśnie IO obarczone indywidualnym obowiązkiem oceny ryzyka stosują tę ocenę w sposób rodzajowy, co pozostaje w sprzeczności z samą ideą systemu AML/CFT. Jest to niejako sytuacja przerzucenia ryzyka na inne podmioty (tego systemu lub występujące poza systemem) poprzez subiektywną ocenę przekroczenia apetytu na ryzyko, a tym samym niedopuszczenie do zarządzania nim w IO.

W zakresie deriskingu i debankingu w wersji przyjętej na tle ustawodawstwa kanadyjskiego można mieć przeświadczenie, że ustalone przez władzę wykonawczą ryzyko (państwowa) jest na tyle wysokie, iż przewyższa ono „apetyt na ryzyko” państwa i w tej sytuacji jego „neutralizacja” następuje przy użyciu IO, które muszą wykonać polecenie władzy wykonawczej. Całość tego typu przedsięwzięć obwarowana jest przepisami ustawy i aktami wykonawczymi. Ten stan rzeczy można określić jako taki, iż władza wyczerpała dotychczasowe środki lub też dotychczasowe środki okazały się bezskuteczne, dlatego postanowiła podjąć tak radykalne rozwiązania w sferze ingerencji w finanse i oszczędności osób rodzajowo określonych jako „protestujący”. W tym przypadku trzeba jednak wskazać, że działania debankingu skupiają się głównie na zamrażaniu aktywów na kontach osób znajdujących się na listach, które instytucjom finansowym dostarczyła policja. Ponadto należałoby zwrócić uwagę na to, że to nadzwyczajne posunięcie związane było także z nowymi sposobami finansowania ulicznych protestów, w drodze tzw. finansowania publicznego określonego jako *crowdfunding*. Zastosowane środki przeciwdziałania miały na celu zablokowanie już zgromadzonych aktywów, uzyskanie obrazu rozpoznania zagrożenia od strony finansowej i przekazanie go agencjom rządowym i bankom w zakresie wymiany „istotnych informacji obejmujących zgłaszanie relacji finansowych z klientami zaangażowanymi w nielegalne blokady”. Prowadziło to do uzyskania szerszego obrazu nie tylko odnośnie do osób fizycznie protestujących, ale także ich inspiratorów, tzw. kibiców, sponsorów, i to zarówno na poziomie krajowym, jak i zagranicznym. Uniwersalność podmiotów, które posiadają status IO (zwłaszcza banki lub kasy oszczędnościowo-pożyczkowe), sprawia, że w nich jak w soczewce kumulują się obowiązki identyfikowane jako *debanking*, choć podstawa do takich działań

znacznie się od siebie różni. Z jednej strony są to przepisy AML/CFT, z drugiej, jak w Kanadzie, przepisy regulujące stany nadzwyczajne i związane z nimi ograniczenie wobec rodzajowo określonych obywateli.

Przykładem zastosowania rodzajowego deriskingu i debankingu wobec zagrożenia bezpieczeństwa mogą być działania J. Trudeau, premiera Kanady, który podjął decyzję, powołując się na ustawę o sytuacjach nadzwyczajnych²³, która obejmuje również rozporządzenie w sprawie nadzwyczajnych środków ekonomicznych ograniczających transakcje finansowe i inne środki, aby stłumić protesty przeciwko nakazowi szczepień poprzez zastosowanie debankingu wobec protestujących. Sam premier, uprzednio wprowadzając stan wyjątkowy, uzasadnił zastosowanie tych przepisów tym, że blokady są „zagrożeniem dla gospodarki i relacji z partnerami handlowymi. Stanowią zagrożenie dla łańcuchów dostaw i dostępności podstawowych towarów, takich jak żywność i leki. Stanowią zagrożenie dla bezpieczeństwa publicznego”²⁴. W konsekwencji bez nakazów sądowych banki mogły zamrozić konta osobiste osób powiązanych z protestami. Ponadto rozszerzono kanadyjskie zasady „finansowania terroryzmu” na kryptowaluty i platformy finansowania społecznościowego. Ustawa o sytuacjach nadzwyczajnych nakazywała instytucjom finansowym zerwanie relacji z niektórymi podmiotami. Korzystając z uprawnień przyznanych na mocy tej ustawy, rząd federalny nakazał bankom i innym instytucjom finansowym zaprzestanie prowadzenia relacji z osobami związanymi z konwojem i mandatem antyszczepionkowym okupującym stolicę kraju²⁵. Misja Freedom Convoy 2022 miała protestować przeciwko wymaganiom kanadyjskiego rządu dotyczącym szczepień przeciwko COVID-19 i przyciągnęła międzynarodową uwagę po tym, jak kierowcy ciężarówek zablokowali most Ambassador między Kanadą a Detroit²⁶.

Zgodnie z rozporządzeniem SOR/2022-22 każdy podmiot wymieniony w sekcji 3²⁷ musiał z chwilą wejścia w życie tego rozporządzenia zakończyć działalność: a) zajmowania się jakimkolwiek mieniem, gdziekolwiek się znajduje, które jest własnością, jest w posiadaniu lub jest kontrolowane, bezpośrednio lub pośrednio, przez wyznaczoną osobę lub przez osobę działającą w imieniu lub pod

²³ S.4619 – Fair Access to Financial Services Act of 2022, <https://www.congress.gov/bills/117/congress/senate-bill/4619/text> (20.04.2024).

²⁴ S. Scherer, D. Ljunggren, J. Gordon, *Canada's Trudeau calls protesters' blockade an economic threat*, Reuters, 18.02.2022; wypowiedź J. Trudeau w Izbie Gmin 18 lutego 2022 r., <https://x.com/JustinTrudeau/status/1494480040192626688?mx=2> (12.01.2025).

²⁵ Emergencies Act, 1988, ustawa o sytuacjach nadzwyczajnych z 1988 r., <https://laws-lois.justice.gc.ca/eng/acts/E-4.5/> (20.04.2024).

²⁶ Usługa crowdfundingowa o nazwie GiveSendGo pozwoliła na przeprowadzenie zbiórki pieniędzy na Freedom Convoy.

²⁷ Emergency Economic Measures Order SOR/2022-22, rozporządzenie z 15 lutego 2022 r. w sprawie nadzwyczajnych środków ekonomicznych: SOR/2022-22, <https://laws-lois.justice.gc.ca/eng/regulations/SOR-2022-22/page-1.html> (20.04.2024).

kierunkiem tej wyznaczonej osoby; b) ułatwiania wszelkich transakcji związanych z handlem, o którym mowa w ust. a; c) udostępniania jakiegokolwiek mienia, w tym funduszy lub wirtualnej waluty, lub na rzecz wyznaczonej osoby lub osoby działającej w imieniu lub pod kierunkiem wyznaczonej osoby; d) świadczenia jakichkolwiek usług finansowych lub powiązanych na rzecz jakiegokolwiek wyznaczonej osoby lub nabywanie takich usług od takiej osoby lub podmiotu lub na rzecz takiej osoby. Wyznaczona osoba oznaczała każdą osobę lub podmiot, który jest zaangażowany, bezpośrednio lub pośrednio, w działalność zabronioną na mocy sekcji 2–5 przepisów dotyczących ustawy o sytuacjach nadzwyczajnych (*personne designée*). Przepisy definiujące „osobę wyznaczoną” umożliwiają odcięcie jej od świadczenia usług finansowych jako osoby, która „bezpośrednio lub pośrednio” uczestniczy w „zgromadzeniu publicznym, co do którego można zasadnie przypuszczać, że doprowadzi do naruszenia porządku publicznego”, lub osoby zaangażowanej w „poważną ingerencję w handel” (*serious interference with trade*) lub „infrastrukturę krytyczną” (*critical infrastructure*). Ponadto podmioty zajmujące się walutą wirtualną i podmioty wykonujące funkcje płatnicze musiały zarejestrować się w Centrum Analiz Transakcji i Raportów Finansowych Kanady (RCMP). Banki również zostały zobowiązane do niezwłocznego ujawnienia „istnienia własności będącej w ich posiadaniu lub kontroli” lub „wszelkich informacji o transakcjach lub proponowanych transakcjach” związanych z „wyznaczoną osobą” zarówno RCMP, jak i Kanadyjskiej Służbie Wywiadu Bezpieczeństwa (CSIS). Przedstawione działania miały charakter administracyjny.

Nakazy nadzwyczajne wymagały od praktycznie każdego uczestnika kanadyjskiego systemu finansowego – banków, firm inwestycyjnych, spółdzielczych kas oszczędnościowo-kredytowych, firm pożyczkowych, maklerów papierów wartościowych, platform pozyskiwania funduszy oraz usług płatniczych i rozliczeniowych – ustalenia, czy posiadają lub kontrolują własność osoby, która uczestniczy w nielegalnym proteście lub zaopatrzeniu demonstrantów. Jeśli znalazły taką osobę na swojej liście klientów, musiały zamrozić jej konta i zgłosić to do RCMP lub kanadyjskim służbom wywiadowczym. Wszelkie podejrzane transakcje należało również zgłaszać do krajowej agencji zajmującej się przeciwdziałaniem praniu brudnych pieniędzy, znanej jako FINTRAC (The Financial Transactions and Reports Analysis Centre of Canada)²⁸.

Debanking (lub ograniczanie ryzyka) pozostaje procesem, któremu brakuje przejrzystości, precyzji i środków prawnych, mimo że może zostać wywołany przez niepotwierdzone lub bezpodstawne zarzuty. To metodyczne podejście władz kanadyjskich z wykorzystaniem debankingu wywołało także szeroką dyskusję w innych krajach angielskojęzycznych, zwłaszcza że FINTRAC nie przedstawiło

²⁸ K. Orland, B. Platt, *Banks get Ottawa protesters' names as financial crackdown gets underway*, 2022, <https://financialpost.com/fp-finance/banking/banks-get-protesters-names-as-canada-financial-squeeze-unfolds> (23.04.2024).

żadnych wskazówek dotyczących rozwiązania tego problemu. Tymczasem jego australijski odpowiednik, Australijskie Centrum Raportów i Analiz Transakcyjnych, zakończyło proces konsultacji, aby zająć się szkodami wynikającymi z procesu debankingu i jego niezamierzonymi konsekwencjami²⁹. Niestety, Kanada ustanowiła nowy precedens prawny, wprowadzając kary zbiorowe za poszczególne przestępstwa. W konsekwencji zawieszono nie tylko osobiste konta bankowe, ale także polisy ubezpieczeniowe, inwestycje i działalność biznesową. Część adresatów była tylko pośrednio, nawet nieświadomie, związana z protestami. Samo zastosowanie debankingu, a jednocześnie powołanie się na przepisy stanów nadzwyczajnych i niejasne kryteria doboru klientów, wobec których miałyby zostać zastosowane środki w postaci zamrażania środków, stały się przedmiotem krytyki. Jak zauważa C.A. Carter: „zamrożenie kont bankowych jest kuszące dla żądnych władzy polityków na całym świecie. Można to zrobić w cieniu, bez publicznego widowiska. Wzbudza to również strach u potencjalnych protestujących, którzy mogą być gotowi zaryzykować aresztowanie za organizowanie się, ale nie mogą ryzykować odcięcia od systemu bankowego. Powoływanie się na kanadyjską ustawę o sytuacjach nadzwyczajnych jest niewłaściwe, jeśli nie grozi wojną lub całkowitym załamaniem społecznym. Zamrażanie kont bankowych jest jeszcze bardziej nielegalne; jest to taktyka państwa policyjnego, na którą nie ma miejsca w demokracji”³⁰. Tym samym zezwolono (a raczej nakazano) bankom na zamrażanie lub zawieszanie kont podejrzanych o udział w nielegalnej działalności bez konieczności uzyskania nakazu sądowego (poza nadzorem sądowym)³¹.

Ponadto możliwe stało się wskazanie innych działań sądowych zmierzających także do uzyskania efektu deriskingu. Sędzia Sądu Najwyższego prowincji Ontario wydał nakaz zamrożenia funduszy o wartości milionów dolarów przekazanych na rzecz Trucker’s Convoy (aktywnego w trakcie protestów), w tym zamrożenia indywidualnych kont bankowych. Nakaz dotyczył głównie tradycyjnego systemu bankowego, ale obejmował również zamrożenie 34 adresów kryptowalut. Stało się to w wyniku obaw, a wręcz strachu nie tylko wobec protestów społecznych, ale także tradycyjnego fiducjarnego systemu finansowego przed systemami finansowymi opartymi na technologii *blockchain* (kryptowalut)³². W konsekwencji zwłaszcza banki starały się niezależnie od nakazów wobec protestujących rodzajowo nie obsługiwać tej kategorii podmiotów. Ponadto obawy koncentrowały się

²⁹ B. Platt, J. Skerritt, *Banks freeze millions in convoy funds under Trudeau edict*, 2022, <https://www.bnnbloomberg.ca/banks-freeze-millions-in-truck-convoy-funds-under-trudeau-edict-1.1727032> (19.04.2024).

³⁰ C.A. Carter, *How Canada Punishes Protesters*, 2022, <https://www.firstthings.com/web-exclusives/2022/03/how-canada-punishes-protesters> (19.04.2024).

³¹ Rząd nakazał zamrożenie szacunkowej kwoty 7,8 mln dolarów na 267 kontach i 170 portfelach Bitcoin sympatyków protestów.

³² S. Klemens, *My 2 Sats: Canada threatens democracy by debanking its own citizens*, 2022, <https://www.exodus.com/news/canada-debanking-citizens/> (19.04.2024).

na tym, że są to szczególne sposoby finansowania crowdfundingu, a więc nie do końca ustalonego celowo finansowania społecznościowego, które może dotyczyć nie tylko przedsięwzięć biznesowych, ale też działań budujących opór i protesty społeczne wobec funkcjonującej władzy³³. Tym samym mogą one być niebezpieczne, ponieważ tego typu rozwiązania można nazwać nie tyle protestami, co „terroryzmem społecznościowym”. Wiadomo, że tradycyjne systemy finansowe pozostają pod stałym nadzorem i związane są z obowiązkiem przeciwdziałania ML/FT, są więc „widoczne” dla władz w kontekście możliwości prowadzenia kontroli, zdobywania wiedzy i zarządzania oddolnymi protestami. W konsekwencji protestujące grupy obywatelskie, posługując się paralelnymi sposobami finansowania tego rodzaju przedsięwzięć, uzyskują swój efekt bez wiedzy czynników państwowych. Obecne modele finansowania paralelnego koncentrują się na powiązaniach: media społecznościowe + *crowdfunding* + kryptowaluty.

Banki w Kanadzie zasadniczo otrzymały listę nazwisk od RCMP (Royal Canadian Mounted Police – Kanadyjska Królewska Policja Konna), jak wyjaśniła przed Komisją Finansów Izby Gmin A. Mason, wiceprzewodnicząca Canadian Bankers Association. Według wiedzy RCMP co najmniej 257 kont zostało zamrożonych przez instytucje finansowe, a RCMP ujawniła informacje o 57 podmiotach instytucjom finansowym i innym wymienionym podmiotom. Ponadto RCMP zidentyfikowała i ujawniła 170 adresów portfeli Bitcoin jako otrzymujących fundusze powiązane z kampanią crowdfundingową Honk Honk Hodl, która zebrała 20,7 Bitcoinów o wartości od 1 mln do 1,2 mln dolarów kanadyjskich w okresie obowiązywania ustawy o sytuacjach nadzwyczajnych³⁴. Kwestia zamrażania środków na rachunkach bankowych oraz zakaz transakcji został

³³ Są to np. upoważnione banki zagraniczne, inne banki, spółdzielcze kasy oszczędnościowo-kredytowych i *caisses populaires* firmy zagraniczne, firmy ubezpieczeniowe w odniesieniu do ich działalności ubezpieczeniowej w Kanadzie, podmioty ubezpieczeń wzajemnych, spółki regulowane ustawą o spółkach powierniczych i pożyczkowych, spółki powiernicze, firmy pożyczkowe, podmioty, które angażują się w działalność w zakresie obrotu papierami wartościowymi lub świadczenie usług w zakresie zarządzania portfelem lub doradztwa inwestycyjnego; podmioty, które zapewniają platformę do pozyskiwania funduszy lub wirtualnej waluty poprzez darowizny, podmioty, które wykonują którąkolwiek z następujących funkcji płatniczych: 1) udostępnianie lub utrzymywanie konta, które w związku z elektronicznym transferem środków jest prowadzone w imieniu jednego lub większej liczby użytkowników końcowych; 2) przechowywanie środków w imieniu użytkownika końcowego do czasu ich wycofania przez użytkownika końcowego lub przekazania ich innej osobie lub podmiotowi; 3) zainicjowanie elektronicznego transferu środków na żądanie użytkownika końcowego; 4) autoryzacja elektronicznego przekazu pieniężnego lub przekazanie, odbiór lub umożliwienie dyspozycji w związku z elektronicznym przelewem pieniężnym; 5) świadczenie usług rozliczeniowych lub rozrachunkowych.

³⁴ *Meeting number 27 of the House of Commons Standing Committee on Finance*, Monday, March 7, 2022, s. 1440, <https://www.ourcommons.ca/DocumentViewer/en/44-1/FINA/meeting-27/evidence> (10.04.2024). Wypowiedź na tym samym posiedzeniu Komisji Michel Arcand (zastępca komisarza, federalnych operacji policyjnych, Królewska Kanadyjska Policja Konna), s. 1605.

rozszerzony także o sprawy związane z zawieszeniem ubezpieczenia pojazdów dla protestujących kierowców ciężarówek, którzy nadal tworzyli blokady, co oznaczałoby, że ten rodzaj zachowań można byłoby określić jako *deinsuranceing*. Zastosowany „epizodycznie” debanking, podporządkowany decyzji władz państwowych, może mieć swoje negatywne konsekwencje w przyszłości. Klienci, którzy zostali naznaczeniu tym epizodycznym debankingiem, będą mogli być negatywnie postrzegani w przyszłości jako podmioty chcące wejść w relacje gospodarcze z IO. Z pewnością będzie to jeden z czynników ryzyka, jaki IO będą brały pod uwagę w odniesieniu do nawiązania relacji (Kanadyjskie Stowarzyszenie Bankierów stwierdziło wręcz, że deponenci mogą być oznaczani dożywotnio).

Inną kwestią jest zamykanie kont dla organizacji społecznościowych związanych z kanadyjską diasporą muzułmańską. Szczegółowy raport zatytułowany *The Untold Story of 'De-banking' in Canada's Muslim Community* autorstwa S. Zhou z National Council of Canadian Muslims (NCCM)³⁵ ujawnił sposób, w jaki konta bankowe wielu organizacji muzułmańskich były zamykane i objęte embargiem. Raport sporządzony dla NCCM prezentuje zdarzenia, w których „banki nakazują meczetom w Kanadzie likwidację lokat na miliony dolarów w ciągu kilku tygodni, a także podjęcie samoistnej inicjatywy zaprzestania przetwarzania darowizn dla dużych muzułmańskich organizacji charytatywnych z niewielkim czasowym wyprzedzeniem”. Wskazano, że decyzje o zamknięciu kont podejmowane wyłącznie przez administracje banków bez nakazu sądowego negatywnie wpływają na globalne działania organizacji muzułmańskich w zakresie pomocy humanitarnej³⁶. Nie sprzyja to racjonalnemu podejściu do zagrożeń wynikających z terroryzmu. Terroryzm w określonym czasie identyfikowany zwłaszcza z organizacjami muzułmańskimi, emanowany poprzez ich relacje z diasporą czy działalność w postaci formalnych organizacji typu NGO (*non-governmental organization*), stał się dużym wyzwaniem dla IO, na które nałożono dodatkowe obowiązki związane z identyfikacją i oceną ryzyka kojarzonego z tego typu podmiotami. Model całkowitej eliminacji klientów w postaci NGO pochodzenia muzułmańskiego nie spowodował efektu ograniczenia ryzyka, a wręcz przeciwnie – mógł jedynie doprowadzić do powrotu przez sprawców do innych alternatywnych sposobów przepływów środków poprzez wykorzystanie systemów *hawala* i podobnych. Stosowanie w tym obszarze debankingu uniemożliwia identyfikację śladów procederu finansowania terroryzmu jak wtedy, gdy byłby on realizowany poprzez instytucje nadzorowane oraz na styku tych instytucji z nienadzorowanymi i nieregulowanymi podmiotami. Zrozumiałe jest, że coraz częściej dla

³⁵ S. Zhou, *Muslim organizations dropped by big banks is a problem*, 2022, <https://news.officialcanada.net/muslim-organizations-dropped-by-big-banks-is-a-problem/> (10.04.2024).

³⁶ S. Aydogan, *Canadian banks target accounts of Muslim institutions "on suspicion of terror financing"*, 2021, <https://www.aa.com.tr/en/americas/canadian-banks-target-accounts-of-muslim-institutions-on-suspicion-of-terror-financing/2680269> (10.04.2024).

bytu wykonawczego NGO niezbędne staje się utworzenie konta bankowego. Islamskie organizacje charytatywne w dużej mierze polegają na internetowych procesorach płatności, przetwarzając miliony darowizn od społeczności. Transakcje te są obsługiwane przez określone firmy, które zwykle współpracują z organizacjami *non-profit*. Główne organizacje muzułmańskie otrzymują miliony darowizn, które są przechowywane w bankach. Potrzebują tych usług, aby przetrwać³⁷.

W konsekwencji tych negatywnych zjawisk nadano w Kanadzie nowe uprawnienia dla Kanadyjskiej Agencji Konsumentów Finansowych (The Financial Consumer Agency of Canada – FCAC), umożliwiające lepszą ochronę klientów w kontaktach z bankami. Nowe uprawnienia FCAC weszły w życie w kwietniu 2020 r. Obejmują one uprawnienia do:

- nałożenia na banki kary w wysokości do 10 mln dolarów za naruszenie ich obowiązków prawnych,
- wprowadzenia nakazu bankom podjęcia działań w celu wywiązania się z ich obowiązków prawnych,
- polecenia bankom poddania się niezależnemu audytowi przeprowadzanemu przez stronę trzecią w celu wywiązania się ze swoich obowiązków prawnych.

Funkcjonowanie debankingu w Meksyku na tle wykluczenia ekonomicznego

Co istotne, *debanking* może wynikać nie tylko z uwarunkowań AML/CFT, politycznych czy uprzedzeń rasowych, ale także z przyczyn ekonomicznych związanych z niskim statusem finansowym mieszkańców. Obecnie ponad 2 mld ludzi na świecie nigdy nie korzystało z usług bankowych. Ludzie ci nie mają dostępu do kont oszczędnościowych, nie mogą też uzyskać pożyczek. Przykładem jest Meksyk. Państwo to jest anomalią zarówno w Ameryce Łacińskiej, jak i wśród innych gospodarek wschodzących, takich jak Kenia i Indie. W tych miejscach odpowiednio 54%, 82% i 80% mieszkańców korzysta z usług bankowych, mimo że Meksyk jest bogatszy. Istnieje kilka powodów, dla których tak niewielu Meksykanów ma dostęp do usług finansowych. Banki są na ogół konserwatywne. CONDUSEF (La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros), organ nadzoru finansowego, twierdzi, że opłaty bankowe w Meksyku są wysokie, a 30% dochodów banków pochodzi z prowizji. Na obszarach wiejskich dostęp do oddziałów może być utrudniony. Co więcej, banki zwykle nie interesują się mniej zamożnymi: tylko jedna piąta z najbiedniejszych 20% Meksykanów posiada konta. Jednocześnie prawie 60% Meksykanów pracuje w sektorze nieformalnym, gdzie mogą otrzymywać dochody w gotówce.

³⁷ S. Zhou, *Muslim organizations...*

Brak dostępu dotyka niektórych bardziej niż innych – biednych, mieszkańców obszarów wiejskich, kobiety i rdzennych mieszkańców. Wyłączenia finansowe na tle zubożałej struktury społecznej mogą, jak uważają ekonomiści, utrudnić ożywienie gospodarcze Meksyku po COVID-19, które zostało stłumione przez brak kontroli nad pandemią. Na przykład małe i średnie firmy zapewniają 95% miejsc pracy w sektorze prywatnym Meksyku, ale tylko 13% z nich ma dostęp do formalnych kredytów³⁸. *Debanking* w Meksyku realizowany jest również w zakresie zamykania rachunków przedsiębiorstw mających siedziby przy granicy amerykańsko-meksykańskiej, co związane jest z nielegalną migracją oraz przestępczością narkotykową.

Zatem przyczyną debankingu może być nieopłacalna obsługa niskodochodowych linii biznesowych dla IO, które służą klientom usługami finansowymi (tym samym dla IO pozostaje wąskie pole do negocjacji ofert). Przy czym o ile uniemożliwienie prowadzenia usług dla klientów z niskim statusem finansowym może zakończyć się prowadzeniem ich obsługi przez małe instytucje płatnicze (MIP; *money service businesses* – MSB), które także są zobowiązane do realizacji obowiązków w ramach system AML/CFT, to w przypadku stosowania deriskingu przez MIP pozostaje klientowi jedynie skorzystanie z nienadzorowanych instytucji finansowych (niebankowych), niejednokrotnie funkcjonujących w szarej lub czarnej strefie gospodarczej. To zaś zwiększa ryzyko zarówno na poziomie ML/FT, ale jak i ryzyko finansowe i gospodarcze. Ponadto wydaje się, że uniemożliwianie podpisywania umów o prowadzenie rachunku bankowego klientom z niskim statusem finansowym może być związane nie tylko z „opłacalnością biznesową”, ale również z tym, że w tego rodzaju obszarach banki mogą postrzegać dodatkowe źródło zagrożenia. Ryzyko może być związane z tym, że klientów takich należałoby także łączyć z nieujawnionymi dodatkowymi dochodami, byciem słupami w większych przedsięwzięciach przestępczych dokonywanych na rynku finansowym, byciem pośrednikiem w uwiarygodnianiu transakcji lub byciem osobowym elementem łańcucha dostaw aktywów na rzecz terrorystów czy też z werbowaniem ich pod względem ideologicznym oraz wykonawczym do ugrupowań terrorystycznych lub do aktywnego udziału w przestępczości zorganizowanej.

Ocena podejścia do debankingu

Wydaje się, że instytucje pokroju banków powinny stanowić forpocztę rozwiązań na potrzeby rozwoju rynku finansowego, gospodarczego czy biznesowego, także w zakresie bezpieczeństwa tych systemów. Jeżeli nie zostaje zachowany

³⁸ *Mexicans lack access to credit*, <https://www.economist.com/finance-and-economics/2020/12/10/mexicans-lack-access-to-credit> (10.04.2024).

balans pomiędzy nieznanym ryzykiem a możliwością jego sfokusowania w „kanały ocenne”, powoduje to sytuację zaprzeczenia idei zapewnienia stabilnego rozwoju rynku finansowego oraz neutralizowania wszelkiego rodzaju zagrożeń społecznych, przestępczych, technologicznych, które temu rozwojowi przeszkadzają. Tym samym stosowanie i intensyfikowanie rozwiązań w zakresie deriskingu i debankingu jako formuły świadomego identyfikowania zagrożeń, wobec których nie dokonuje się oceny ryzyka, a releguje się je z relacji z instytucją bankową czy inną IO, jest samym w sobie zagrożeniem dla bezpieczeństwa zarówno tej instytucji, jak i innych podmiotów świadczących podobne usługi.

Nie jest właściwe spojrzenie, że w związku z tym, iż banki nie są mimo posiadania statusu podmiotu zaufania publicznego lubiane przez swoich klientów i wiąże je z nimi jedynie wymuszona relacja, to stanowi to podstawę do usprawiedliwienia tworzenia bytów debankingu w praktyce. Co istotne, taki model postępowania instytucji finansowych czy mających status niefinansowej IO przechodzi na akty wykonawcze podmiotów rządowych jako element przeciwdziałania zagrożeniom wywoływanym przez grupy społeczne zaburzające porządek publiczny. Niestety *debanking* staje się też instrumentem walki na tle rasowym czy narodowościowym. Występujący współcześnie trend do poszerzania takiego podejścia również na inne obszary społeczne (np. wynajem nieruchomości, gdzie najemcy odmawiają podpisania umowy wynajmu z powodu małych dochodów albo żądają bardzo wysokich kaucji zabezpieczających, dotyczy np. wynajmu mieszkań w Londynie dla Polaków jako określonej narodowości). Coraz trudniej jest więc rozgraniczyć kwestię „pozytywnego” debankingu, realizowanego na potrzeby rzeczywistego bezpieczeństwa, z „negatywnym” debankingiem, działającym z pobudek subiektywnych, braku zasobów indywidualnych czy słabości kadry *compliance* i AML/CFT lub też wynikającym z nierozumienia rozwoju technologicznego rynku inwestorskiego.

Debanking w rzeczywistości jest błędnym zastosowaniem podejścia opartego na ryzyku. Z założenia „rynek finansowy” posiada charakter dynamiczny, tym samym takie IO jak banki powinny być odporne na negatywne czynniki, ale także dominujące w rozpoznawaniu nowych tendencji/trendów i powstających instytucji gospodarczych. Ich pozycja społeczna i instrumentarium działań stawia je w innej roli, która powinna się koncentrować na inicjatywie regulacyjnej, a nie na odrzucaniu czy niezabezpieczaniu pola zagrożenia. Nietrudno też zauważyć, że sam schemat debankingu zapętla się sam w sobie. Odrzucenie wchodzenia w relacje z firmami Fintech (np. start-upy) powoduje, że te poszukują innych sposobów finansowania, zwłaszcza tzw. finansowania społecznościowego, głównie poprzez *crowdfunding*. Oba te rodzaje podmiotów i sposobów inwestowania często stają się przedmiotem debankingu. Tym samym potrzebując się aktywizować, muszą tworzyć paralelne sposoby funkcjonowania, niekiedy powiązane z równoległymi „walutami”, jak Bitcoin, czyli do już wskazanych dochodzi dodatkowy przedmiot debankingu. W konsekwencji banki tracą klientów, których mogłyby obsługiwać,

tracą bycie partnerem inwestycyjnym wobec nowoczesnych technologii i relacji społecznych, a same podmioty będące przedmiotem odrzucenia budują równolegle sieci relacji finansowo-inwestycyjno-biznesowych, w których banki nie uczestniczą.

W konsekwencji takie działania banków nie ułatwiają poszukiwania śladów podejrzanych klientów czy transakcji zarówno dla jednostek analityki finansowej, jak i dla organów ścigania. Ten skutek natomiast posiada bezpośrednie przełożenia na bezpieczeństwo publiczne. Dlatego też banki odgrywające istotną rolę w zakresie zapewniania bezpieczeństwa finansowego i gospodarczego zarówno w skali indywidualnego klienta, jak i państw nie przyczyniają się wobec stosowania praktyk debankingu do zapewniania bezpieczeństwa, izolując się wobec określonych subiektywnie potencjalnych klientów czy obszarów geograficznych. Tracą także atut (status) posiadanej pozycji i instrumentów wykonawczych na potrzeby kreowania „bezpiecznego obszaru inwestowania” zarówno dla podmiotów krajowych, jak i zagranicznych. W konsekwencji do relacji gospodarczych może wchodzić kapitał spekulacyjny i aktywa pochodzące z czarnej lub szarej strefy gospodarczej.

W przedmiotowych działaniach należałoby wyróżnić dwa kierunki postępowania. Pierwszy związany jest z inicjatywą samych IO. W tym zakresie prowadzą one własną politykę oceny ryzyka i odstępowania od zarządzania nim. Przyznanie instytucjom swobody w tworzeniu własnych zasad AML/CFT oznacza również większe prawdopodobieństwo różnic w interpretacji i osądach pomiędzy IO a organami nadzoru – sytuacja ta naraża instytucje na znaczne niebezpieczeństwo, jeśli nie zastosują prawidłowo podejścia opartego na ryzyku do swoich spraw³⁹. Jest to kierunek oddolnego postępowania z ryzykiem. Drugi odnosi się do narzucania określonych rozwiązań na IO, co związane jest z możliwościami, jakie dają przepisy władzy wykonawczej. W tym zakresie „oceny” ryzyka dokonują inne niezależne od IO podmioty, a instytucje jedynie wykonują ich wolę. Tym samym element debankingu może być wynikiem samoregulacji i samooceny IO lub też jedynie w podobnym zakresie przedmiotem wykonania decyzji podmiotu zewnętrznego, pośrednio przy wykorzystaniu organów nadzorczych (jednostek analityki finansowej). W konsekwencji te „czynniki wykreowanego ryzyka” stają się elementem wewnętrznej polityki bezpieczeństwa nie tyle IO, co np. organów władzy państwowej (także spoza systemu AML/CFT). Oba tego typu podejścia kierunkowe mogą świadczyć o słabości jednostek analityki finansowej i ich instrumentalnym wykorzystaniu. W konsekwencji niezbędne wydaje się podjęcie kolejnych inicjatyw ustawodawczych zapewniających gwarancje obywatelskie wobec przedstawionych rozwiązań podejmowanych pod pretekstem eliminacji ryzyka związanego z bezpieczeństwem.

³⁹ M. Nilsson, E. Shorroch, *Debanking and the Law of Unintended Consequences*, 2019, <https://www.kroll.com/en/insights/publications/financial-compliance-regulation/global-regulatory-outlook-2019/debanking-and-the-law-of-unintended-consequences> (19.04.2024).

Podsumowanie

Początkowo wąskie dość pojęcie *debanking* z czasem rozprzestrzeniło się na różne uwarunkowania społeczne. Jedynym spójnym elementem, który pozostał, jest działanie instytucji produkto- i usługodawczych poprzez wykluczenie określonych kategorii klientów. W związku z tym można wyróżnić różnego rodzaju powody do działań mieszczących się w pojęciu *debanking*. Do tych obszarów można zaliczyć:

- podejmowanie działań subiektywnych, wykluczających pod pretekstem wykonywania (niewłaściwego) obowiązków wynikających z podmiotowości, bycia podmiotem o statusie IO w systemie przeciwdziałania ML/FT wobec określonego rodzaju klientów, zwłaszcza rodzących wysokie ryzyko,
- podejmowanie w IO działań wykluczających wynikających z braku możliwości realizacji i wdrożenia środków bezpieczeństwa finansowego,
- wykluczenie jako *a priori* postępowanie powodowane brakiem możliwości (nawet przy ustalonej identyfikacji) skali ryzyka instytucjonalnego (zwłaszcza) czy indywidualnego,
- wykluczenie mające podstawy w niskim statusie materialnym potencjalnych klientów, a tym samym obawie spłaty uzyskanych środków z instytucji bankowych,
- wykluczenie realizowane jako wynikające z uprzedzeń na tle rasowym, religijnym, narodowościowym, koloru skóry, odmienności seksualnej,
- wykluczenie wynikające z realizacji sankcji wobec podmiotów wyznaczonych jako związane z działalnością terrorystyczną, uprzednio umieszczonych na listach sankcyjnych,
- wykluczenie narzucone instytucjom bankowym przez władze państwową jako element realizacji nakazu z woli państwowych organów wykonawczych, będącego instrumentem represji wobec społeczeństwa.

Mając na uwadze, że identyfikacja klienta poprzez stosowanie środków bezpieczeństwa finansowego może być realizowana także za pomocą zgodności danych biometrycznych, możliwe będzie również zwrócenie uwagi na tę kwestię w zakresie stosowania *debankingu*. Na sprawę wykluczenia przy biometrii zwrócił uwagę J. Lunter⁴⁰ w swoim artykule *Synthetic data: a real route to eliminating bias in biometrics*. Zauważył on, że jedną z najbardziej oczywistych potencjalnych korzyści płynących z danych syntetycznych w szkoleniu algorytmów biometrycznych jest zrównoważenie zestawów danych szkoleniowych, które składają się w nieproporcjonalnym stopniu z białych mężczyzn, co prowadzi do rozbieżności demograficznych lub „stronniczości”. Dobór biometryczny w zbiorach uczących może więc okazać się kolejnym instrumentem realizującym *debanking* na poziomie IO posługujących się identyfikacją biometryczną jako środkiem bezpieczeństwa finansowego.

⁴⁰ J. Lunter, *Synthetic data: a real route to eliminating bias in biometrics*, „Biometric Technology Today” 2023, no. 1, <https://www.magonlinelibrary.com/doi/full/10.12968/S0969-4765%2823%2970001-5> (10.04.2024).

Uwzględniając powyższe rozważania i przyjmując, że *derisking/debanking* jest jakąkolwiek metodą (raczej nie naukową, a wykonawczą/praktyczną), czyli sposobem do neutralizacji problemu ryzyka w IO, należałoby uznać, że tego typu postępowanie pozostaje zaprzeczeniem wyjaśnienia problemu ryzyka w zakresie AML/CFT, jeżeli jest podejmowane wobec określonej rodzajowo i zespołowo społeczności. Postępowanie takie jest natomiast dopuszczalne, jeżeli jest poprzedzone identyfikacją i oceną ryzyka w poszczególnym indywidualnym przypadku. W tej drugiej sytuacji *derisking/debanking* znajduje uzasadnienie ze względu na niemożliwość zastosowania określonych środków bezpieczeństwa finansowego, a tym samym wyzbycia się ryzyka IO, zwłaszcza przy braku współdziałania ze strony klienta tej instytucji. Tym samym *derisking/debanking* jest dopuszczalną metodą postępowania zmierzającą do neutralizacji ryzyka AML/CFT, ale w prawem określonych sytuacjach i gdy IO postępuje w sposób uzasadniony indywidualnie (wskazuje na to np. wynik dokonanej oceny ryzyka oraz występowanie dodatkowych czynników negatywnych określonych przepisami ogólnymi). Wydaje się jednak, że samo zastosowanie *deriskingu/debankingu* w IO nie „załatwia” problemu ryzyka, jeżeli nie zostanie to postępowanie powiązane z innego rodzaju czynnościami, np. takimi, jak segmentacja klienta, zakwalifikowanie sytuacji do podejrzanej, o której należałoby powiadomić jednostkę analityki finansowej w postaci raportu SAR (*A Suspicious Activity Report*, raport o podejrzanych działaniach) lub STR (*A Suspicious Transaction Report*, raport o podejrzanych transakcjach). W polskim ustawodawstwie są one określone niemożnością wykonania procedury (art. 41 ust. 1 u.p.p.p.f.t.) oraz dodatkowo podejrzalnością wiązaną z klientem i transakcją (art. 41 ust. 1 w zw. z ust. 2 i art. 74 lub art. 86 u.p.p.p.f.t.).

Podobnie należałoby postępować w przypadku zastosowania „mechanizmu *deriskingu*” w innych obszarach niż AML/CFT, jednak bez używania argumentacji przynależnej temu charakterystycznemu obszarowi przeciwdziałania. System AML/CFT nie powinien służyć do eliminowania ryzyka związanego z przynależnością kulturową, religijną, rasową czy ekonomiczną, a zgodnie z przyjętym celem – przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Podobieństwo więc może być pozorne, ale nie wypełnia celowościowej roli *deriskingu* systemu AML/CFT. Rynek finansowo-gospodarczy i zjawisk społecznych co jakiś czas jest narażany na różnego rodzaju zagrożenia związane najczęściej z aktualnym rozwojem technologicznym i chęcią dominacji. Mając na uwadze cele systemu AML/CFT, niezwykle ważne jest więc to, aby uczestnicy relacji zachowali równowagę między zapewnieniem bezpieczeństwa i integralności systemu a zachowaniem otwartości wobec nowych zjawisk, niekoniecznie wiążących się wyłącznie z przestępczością. Oprócz siły państwa także siła niektórych IO, w tym głównie banków, powinna wykreować postawy metodycznego badania zagrożenia, chociażby w oparciu o ocenę ryzyka, a nie wyzbywać się globalnie tego rodzaju problemów. Wszakże rugowanie go z własnej przestrzeni jako nierozwiązanego świadczy o słabości instytucjonalnej i nadaje zagrożeniu nowego niebezpiecznego wymiaru poza kontrolą

państwa i poza kontrolą systemów bezpieczeństwa finansowego. Wydaje się, że występuje tu także przyczynowe balansowanie pomiędzy podejściem „subiektywnym” a „obiektywnym”. Z pierwszego korzystają IO poprzez własne polityki bezpieczeństwa, a w konsekwencji dyskredytowanie finansowe określonego rodzaju podmiotów – w ich ocenie „nieodpowiednich”. Drugie zaś związane jest z budowaniem oceny obiektywnej przez organy władzy, które tworząc centralną politykę bezpieczeństwa, przekładają ją na wykonawstwo dla IO. Skrajne przypadki podejść tych dwóch typów ocen i deeskalacji zagrożeń mogą powodować zdarzenia generujące dodatkowe niebezpieczne czynniki bez neutralizacji dotychczasowych. Wydaje się więc istotne przyjęcie trzeciego rozwiązania, które będzie polegało na wzajemnym „kontrolowaniu” się zarówno instytucji finansowych, jak i organów władzy⁴¹.

System AML/CFT musi zatem wykreować schematy przeciwdziałania, również wychodząc naprzeciw innowacyjnym rozwiązaniom, nawet gdy jakaś ich część może być wykorzystana w sposób niezgodny z prawem, a może zwłaszcza dlatego.

Bibliografia

- Aydogan S., *Canadian banks target accounts of Muslim institutions “on suspicion of terror financing”*, 2021, <https://www.aa.com.tr/en/americas/canadian-banks-target-accounts-of-muslim-institutions-on-suspicion-of-terror-financing/2680269> (10.04.2024).
- Carter C.A., *How Canada Punishes Protesters*, 2022, <https://www.firstthings.com/web-exclusives/2022/03/how-canada-punishes-protesters> (19.04.2024).
- Klemens S., *My 2 Sats: Canada threatens democracy by debanking its own citizens*, 2022, <https://www.exodus.com/news/canada-debanking-citizens/> (19.04.2024).
- Lemieux M., *De-banking international money remitters in Canada*, 2018, <https://www.linkedin.com/pulse/de-banking-international-money-remitters-canada-marc-lemieux> (14.05.2024).
- Lunter J., *Synthetic data: a real route to eliminating bias in biometrics*, „Biometric Technology Today” 2023, no. 1, <https://www.magonlinelibrary.com/doi/full/10.12968/S0969-4765%2823%2970001-5> (10.04.2024).
- Meeting number 27 of the House of Commons Standing Committee on Finance*, Monday, March 7, 2022, <https://www.ourcommons.ca/DocumentViewer/en/44-1/FINA/meeting-27/evidence> (10.04.2024).
- Mexicans lack access to credit*, <https://www.economist.com/finance-and-economics/2020/12/10/mexicans-lack-access-to-credit> (10.04.2024).
- Nilsson M., Shorrock E., *Debanking and the Law of Unintended Consequences*, 2019, <https://www.kroll.com/en/insights/publications/financial-compliance-regulation/global-regulatory-outlook-2019/debanking-and-the-law-of-unintended-consequences> (19.04.2024).

⁴¹ Przykładem jest decyzja Komisji Bankowości miasta Nowy Jork, która zadecydowała, w jakich bankach umieścić fundusze miejskie na kolejne lata. Jednym z czynników decydujących była ocena polityki dyskryminacyjnej. Głosowano przeciwko trzem bankom składającym wniosek – International Finance Bank, PNC Bank i Wells Fargo – ponieważ ich wnioski nie wskazywały na wystarczające wysiłki antydyskryminacyjne przy podejmowaniu decyzji kredytowych, otwieraniu i zamykaniu oddziałów oraz innych operacjach. D. Turetsky, *City Limits: In a First, the Public Got to Weigh in on NYC’s Banking Decisions*, <https://www.neweconomynyc.org/2023/06/city-limits-in-a-first-the-public-got-to-weigh-in-on-nycs-banking-decisions/> (16.05.2024).

- Orland K., Platt B., *Banks get Ottawa protesters' names as financial crackdown gets underway*, 2022, <https://financialpost.com/fp-finance/banking/banks-get-protesters-names-as-canada-financial-squeeze-unfolds> (23.04.2024).
- Platt B., Skeritt J., *Banks freeze millions in convoy funds under Trudeau edict*, 2022, <https://www.bnnbloomberg.ca/banks-freeze-millions-in-truck-convoy-funds-under-trudeau-edict-1.1727032> (19.04.2024).
- Scherer S., Ljunggren D., Gordon J., *Canada's Trudeau calls protesters' blockade an economic threat*, Reuters, 18.02.2022.
- The Somali Remittance Crisis: when remittances are needed the most*, <https://crosstechpayments.com/somalian-remittance-crisis/> (20.04.2024).
- Turetsky D., *City Limits: In a First, the Public Got to Weigh in on NYC's Banking Decisions*, <https://www.neweconomy.org/2023/06/city-limits-in-a-first-the-public-got-to-weigh-in-on-nycs-banking-decisions/> (16.05.2024).
- Wald E.R., *Debanking Hurts Everyone*, 2021, <https://www.barrons.com/articles/debanking-hurts-everyone-51610145010> (10.05.2024).
- Zhou S., *Muslim organizations dropped by big banks is a problem*, 2022, <https://newsocanada.net/muslim-organizations-dropped-by-big-banks-is-a-problem/> (10.04.2024).
- Zywicki T., *Restoring the Rule of Law in Finance*, „First Principles” 2023, no. 92, <https://www.heritage.org/sites/default/files/2023-06/FP92.pdf> (17.05.2024).

Streszczenie

Założenia systemu AML/CFT preferowały oddolną inicjatywę instytucji obowiązanych w zakresie oceny ryzyka instytucji oraz indywidualnego klienta. Z czasem wobec takiego stanu rzeczy wykształciła się negatywna praktyka eliminacji ryzyka w postaci deriskingu i debankingu. Polega ona na unikaniu oceny ryzyka poprzez zbiorowe i rodzajowe niedopuszczanie do zawierania umów z określonymi klientami i rozwiązywania umów już zawartych. Ten stan rzeczy nie neutralizuje ryzyka, a jedynie przesuwają go na inne obszary do podmiotów, które słabiej identyfikują to ryzyko. *Derisking/debanking* mimo negatywnej oceny rozszerzył się także na inne obszary społeczne poza AML/CFT. Jednocześnie stał się on elementem wykorzystywanym w dyskryminacji ze względu na warunki ekonomiczne, rasowe, pochodzenie narodowe.

Słowa kluczowe: derisking, debanking, pranie pieniędzy, finansowanie terroryzmu, sankcje, ryzyko

DERISKING/DEBANKING AS “METHODS” OF PROVIDING SECURITY?

Summary

The assumptions of the AML/CFT system favored the bottom-up initiative of mandatory institutions in assessing the risk of the institution and the individual customer. Over time, in view of this state of affairs, the negative practice of risk elimination in the form of derisking and debanking has developed. It consists of avoiding risk assessment through collective and generic disallowance of contracts with specific customers and termination of contracts already concluded. This state of affairs does not neutralize the risk but only shifts it to other areas to entities that are weaker in identifying the risk. *Derisking/debanking*, despite its negative assessment, has also expanded into other areas of society beyond AML/CFT. At the same time, it has become an element used in discrimination based on conditions: economic, racial, national origin.

Keywords: derisking, debanking, money laundering, terrorist financing, sanctions, risk