

Warszawa, dnia 27 marca 2024 r.

Dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ASzWoj  
Katedra Prawa Informatycznego  
Wydział Prawa i Administracji  
Akademia Sztuki Wojennej

**Recenzja rozprawy doktorskiej pani mgr Caroli Bader <sup>1</sup>**  
**pt. „Pranie pieniędzy i finansowanie terroryzmu -zadania i obowiązki sektora**  
**finansowego w systemie globalnym”<sup>2</sup>**

**I. Kryteria oceny**

Kryteria oceny osiągnięć osoby ubiegającej się o nadanie stopnia doktora zostały określone w art. 186 ust. 1 pkt 4 ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2023 r. poz. 742 z późn. zm.). Zgodnie z art. 186 ust. 1 pkt 4, ww. ustawy przedmiotem recenzji jest maszynopis rozprawy doktorskiej zatytułowanej „*Pranie pieniędzy i finansowanie terroryzmu -zadania i obowiązki sektora finansowego w systemie globalnym*”.

**II. Przedmiot oceny**

Pani mgr Carola Bader przedstawiła do oceny w przewodzie doktorskim osiągnięcie naukowe stanowiące rozprawę pt. „*Pranie pieniędzy i finansowanie terroryzmu - zadania i obowiązki sektora finansowego w systemie globalnym*”.

**III. Ocena osiągnięcia naukowego – rozprawy pt. „Pranie pieniędzy i finansowanie terroryzmu -zadania i obowiązki sektora finansowego w systemie globalnym”.**

***1. Temat i zakres pracy***

Przestępczość finansowa stanowi dziś globalne wyzwanie dla biznesu i społeczeństwa. szczególności pranie pieniędzy i finansowanie terroryzmu stanowią poważne zagrożenie dla systemu finansowego, a także dla bezpieczeństwa jednostkowego oraz globalnego. Jak zauważa Doktorantka, przestępstwa finansowe, takie jak pranie pieniędzy i finansowanie terroryzmu, stanowią wielowymiarowe zagrożenie, które wykracza poza sektor finansowy i obejmuje szersze spectrum społeczno-gospodarcze. Tego typu nielegalne działania nie tylko podważają integralność rynku, ale mogą również wpływać na relacje między przedsiębiorcami i sytuację rynkową, w szczególności jeśli dochodzi do wzmożonej aktywności zorganizowanych grup przestępczych.

---

<sup>1</sup> Podstawa sporządzenia recenzji:

- 1) Wszczęcie przewodu doktorskiego na podstawie uchwały Rady Naukowej Instytutu Prawa SWPS Uniwersytetu Humanistycznospołecznego.
- 2) Powołanie w skład Komisji w charakterze recenzenta uchwałą Rady Naukowej Instytutu Prawa SWPS Uniwersytetu Humanistycznospołecznego zgodnie z art. 190 ust. 2 Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742 z późn. zm.).

<sup>2</sup> Tytuł oryginału w języku angielskim: **Money Laundering and Terrorist Financing – Tasks and Obligations of the Financial Sector in a Global System.**

Poziom przestępczości i korupcji może wpływać na gospodarkę, a przestępcy uzyskują wpływ na politykę i sytuację finansową danego państwa. Wynikająca z tego utrata zaufania konsumentów i zwiększone wydatki publiczne na egzekwowanie prawa, dodatkowo obciążają zasoby społeczne. Ponadto te przestępstwa i związane z nimi inwestycje mają zniekształcający wpływ na zmienne makroekonomiczne, takie jak stopy procentowe i kursy wymiany walut, a także ułatwiają uchylanie się od płacenia podatków, co skutkuje znacznymi stratami dochodów państwa, co ma wpływ na jakość i poziom realizacji zadań publicznych oraz celów interesu publicznego. Zdaniem Doktorantki, przestępczość finansowa wpływa na dynamikę rynku, struktury zarządzania i zaufanie społeczne oraz podważa ogólną stabilność gospodarczą. Problem ten stał się elementem dyskursu na poziomie międzynarodowym i krajowym w celu wypracowania rozwiązań służących zwalczaniu tych przestępstw. W świetle takich uwarunkowań, także wobec coraz nowocześniejszych metod działania tego typu terrorystów, podjęcie tego rodzaju tematyki wydaje się niezwykle potrzebne, a systemowe, regulacyjne podejście do tego problemu - niezwykle nowatorskie. Wielu zagadnień na obecnym etapie nie da się rozwiązać, jednak bez prac badawczych, obejmujących diagnozę obecnego stanu i identyfikację potrzeb, trudno jest podejmować działania naprawcze. Wybór omawianej w pracy problematyki należy zatem uznać za trafny.

## ***2. Kompozycja pracy***

Konstrukcja pracy jest przejrzysta i odpowiada jej tematowi. Doktorantka dokonała podziału rozprawy, w ramach którego łącznie znajduje się pięć rozdziałów, podzielonych na mniejsze jednostki redakcyjne. Pracę wieńczy rozdział szósty, który jednocześnie stanowi podsumowanie zawierające konkluzje i wnioski.

Przedstawiona do oceny rozprawa liczy 157 stron tekstu merytorycznego, a nadto: spis treści i zestawienie literatury. Objętość poszczególnych części jest względnie zrównoważona i symetryczna, zarówno pod względem liczby stron, jak i wewnętrznego podziału każdej części.

## ***3. Strona warsztatowa***

Generalnie strona warsztatowa pracy nie budzi zastrzeżeń. Doktorantka kompetentnie posługuje się językiem prawniczym, ponadto przeprowadza analizę źródeł. Wywody należy uznać za precyzyjne i konsekwentne. Bibliografia obejmuje imponujące 424 pozycje razem ze źródłami prawa i dokumentami strategicznymi, przy czym są to najważniejsze pozycje związane z podejmowaną tematyką, przytoczona literatura jest bardzo obszerna. Dodatkowo Doktorantka posłużyła się źródłami internetowymi. Metodologia, opisana w rozdziale pierwszym rozprawy, ma na celu zapewnienie kompleksowego i krytycznego zrozumienia

wielowarstwowej złożoności przestępstw finansowych, ze szczególnym uwzględnieniem prania pieniędzy i finansowania terroryzmu.

Na potrzeby rozprawy Doktorantka podzieliła pracę na trzy główne sekcje tematyczne, które jak twierdzi, zostały wykorzystane w celu uelastycznienia podejścia analitycznego. W związku z tym sugerowane kierunki rozwojowe są także podzielone na trzy, aby umożliwić kompleksowe podejście do skutecznych ram przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Ponadto badanie oparto na obszernym przeglądzie literatury, istniejących publikacji akademickich, a także przepisów ustawowych, dyrektyw, rozporządzeń, konwencji, rezolucji, wytycznych i zaleceń na szczeblu krajowym i międzynarodowym dotyczących zwalczania prania pieniędzy i finansowania terroryzmu. Dodatkowo w pracy uwzględniono odpowiednie raporty oraz publikacje instytucji międzynarodowych, takich jak FATF, ONZ lub UE, oraz instytucji krajowych, w tym Federalnego Urzędu Nadzoru Finansowego (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) w Niemczech oraz Jednostki Analityki Finansowej (FIU), które zapewniają odpowiedni wgląd w te zjawiska, znalazło się miejsce na rzeczywiste studia przypadków.

Kompleksowa analiza i ocena istniejącej wiedzy na temat prania pieniędzy i finansowania terroryzmu pozwoliła Doktorantce na przeglądowe zrozumienie tematu oraz identyfikację powtarzających się zagrożeń i obecnych środków zaradczych w różnych źródłach danych. Podejście to wspiera zatem główny cel, jakim jest krytyczna ocena obecnej sytuacji w zakresie prania pieniędzy i finansowania terroryzmu w Niemczech w warunkach konieczności wypełnienia tych luk poprzez ocenę skutecznych podejść do zwalczania prania pieniędzy i finansowania terroryzmu.

Natomiast wydaje się, że nie został prawidłowo i wystraszająco uzasadniony przez Doktorantkę wybór przykładu niemieckiego, który zaprezentowano w postaci całego, wyodrębnionego rozdziału rozprawy. Temat pracy dotyczy sytuacji globalnej i chociaż Doktorantka przedstawia tło ogólnoświatowe, to jednak w dużym stopniu skupia uwagę na sytuacji w Niemczech, co powoduje pewną nieproporcjonalność w stosunku do podjętej tematyki. Podatność kraju na pranie pieniędzy i finansowanie terroryzmu jest zwiększona przez duży nieformalny sektor, powszechne korzystanie z gotówki, uchylanie się od płacenia podatków, a także obecność zagranicznych organizacji terrorystycznych, ich sympatyków i bojowników, dlatego uznaje Niemcy jako przypadek szczególny, co trudno uznać za oczywiste, a teza ta wymagałaby uzasadnienia popartego większą liczbą danych. Doktorantka podkreśla, iż Niemcy mają zdecydowanie największą liczbę instytucji kredytowych w strefie euro i ich oddziałów zagranicznych w porównaniu z innymi państwami członkowskimi UE. Główne

banki komercyjne oferują szeroki zakres międzynarodowych usług finansowych. Co więcej, Niemcy są siedzibą jednej z największych na świecie giełd papierów wartościowych, Frankfurckiej Giełdy Papierów Wartościowych, i mają duży sektor ubezpieczeniowy, który jest ściśle powiązany z sektorem bankowym. Niemcy zajmują siódme miejsce w Indeksie Tajności Finansowej 2022, co wskazuje na wyraźną podatność na pranie pieniędzy i finansowanie terroryzmu. W świetle tych czynników, zdaniem Doktorantki konieczne było przeprowadzenie analizy sytuacji w tym kraju pod względem zagrożeń praniem pieniędzy i finansowaniem terroryzmu w celu opracowania odpowiednich środków zwalczania i ograniczania tych przestępstw. Jednak wskazane tu uwarunkowania, w moim przekonaniu, nie są wystarczającym argumentem. Rozdział piąty rozprawy koncentruje się na krytycznej analizie zagrożeń i podatności Niemiec na pranie pieniędzy i finansowanie terroryzmu. Doktorantka wskazuje na wiodącą europejską potęgę gospodarczą, strategiczne położenie Niemiec, dużą gospodarkę, otwarte granice, otwarte centrum finansowe i rozległe powiązania międzynarodowe, które sprawiają, że Niemcy są kluczowym graczem w walce z przestępczością finansową. Być może wobec tak zaprezentowanych uwarunkowań, tytuł całej pracy powinien nawiązywać do przypadku niemieckiego.

Rozprawa kończy się prezentacją wniosków i zaleceń. Ponieważ analiza wykracza poza istniejące ramy prawne i bada potencjalne ulepszenia, badania kończą się zestawem zaleceń mających na celu wzmocnienie istniejących ram prawnych, poprawę mechanizmów egzekwowania prawa i zacieśnienie współpracy między zainteresowanymi stronami zaangażowanymi w walkę z praniem pieniędzy i finansowaniem terroryzmu. Poprzez syntezę i analizę badanie przeprowadzone w rozprawie miało na celu zaprezentowanie problematyki w świetle istniejącego zasobu wiedzy i wyznaczenie kierunków kształtowania przyszłej polityki w obszarze przestępstw finansowych o podłożu terrorystycznym, co zostało osiągnięte w satysfakcjonującym zakresie.

#### ***4. Treść merytoryczna***

Podjęte zadanie badawcze Doktorantka wykonała w sposób zadowalający, przedstawiając merytorycznie poprawną rozprawę doktorską. Na podkreślenie zasługują obszerne nawiązania do literatury krajowej oraz przegląd rozwiązań zagranicznych, ciekawych źródeł internetowych, nie odnosząc się jednak do konkretnych sytuacji w innych państwach działających globalnie w pozaeuropejskich i poza amerykańskich systemach prawnych, co po uzupełnieniu niewątpliwie wzbogacałoby przeprowadzony wywód. W tym kontekście przeanalizowano instrumenty stosowane przez globalne podmioty, takie jak Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF), Organizacja Narodów Zjednoczonych (ONZ) i

Organizacja Współpracy Gospodarczej i Rozwoju (OECD), a także rozwiązania obowiązujące w Stanach Zjednoczonych, Unii Europejskiej (UE) i w Niemczech. W odniesieniu do tego ostatniego państwa trudno przyjąć jednak jako oczywiste stanowisko, że w świetle globalnej sytuacji, Niemcy są szczególnie narażone na przestępstwa finansowe ze względu na swoją wiodącą gospodarkę, otwarte granice, centrum finansowe i dużą ilość gotówki w obiegu.

Doktorantka w sposób interesujący wskazuje na istnienie kilku istotnych definicji prania pieniędzy i finansowania terroryzmu. Przeprowadza kompleksowy podział cyklu prania pieniędzy, wyodrębniając jego etapy lokowania, nawarstwiania i integracji oraz etapy, które obejmują gromadzenie, przechowywanie, przemieszczanie i wykorzystywanie funduszy. Ponadto zauważa, że istnieją wzajemne powiązania między praniem pieniędzy i finansowaniem terroryzmu, a także różnice w pochodzeniu i ostatecznym przeznaczeniu funduszy oraz ramach czasowych nielegalnej działalności, co stanowi bardzo ciekawe podejście do prezentowanej tematyki. Doktorantka prezentuje to jako podstawową tezę pracy.

W świetle powyższych założeń, zadanie badawcze postawione przez Doktorantkę dotyczy odpowiedzi na istotne pytanie o przyszłe mechanizmy rozwiązań dotyczących zwalczania terroryzmu i źródeł jego finansowania. Biorąc pod uwagę dynamiczny i złożony charakter przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, Doktorantka zdecydowała się na wykorzystanie w pracy modelu zarządzania zmianą do analizy i zaproponowania możliwych rozwiązań w obszarze transformacji. W szczególności zastosowała model Kottera, który służy jako podstawa teoretyczna dla strukturyzacji proponowanych przyszłych rozwiązań. Model Kottera przedstawia ośmioetapowy proces skutecznej zmiany, który jest często agregowany w trzech głównych fazach, z których wobec obszaru badawczego najistotniejsze są ustalenia prawne. Co ciekawe, konsekwentnie i w podobny sposób Doktorantka buduje system swoich rozważań. W kontekście przekazu danych, które są obecnie poza zakresem pełnego dostępu – Doktorantka podkreśla potrzebę podążania w kierunku integracji w walce z terroryzmem, co zapewni organom terminowy dostęp do potrzebnych danych, takich jak informacje podstawowe lub informacje o beneficjentach rzeczywistych, zgodnie ze standardami FATF<sup>3</sup>. Ponadto Doktorantka wskazuje, że działania legislacyjne powinny być regularnie poddawane przeglądowi w celu potwierdzenia ich adekwatności i spójności z zaleceniami FATF.

---

<sup>3</sup> Grupa Zadaniowa ds. Przeciwdziałania Praniu Pieniędzy, znana również pod francuską nazwą Groupe d'action financière, jest organizacją międzyrządową założoną w 1989 r. z inicjatywy G7 w celu opracowania polityki zwalczania prania pieniędzy i utrzymania pewnych interesów.

Korzystając z postępu technologicznego, zdaniem Doktorantki istniejące rejestry powinny zostać skonsolidowane i zsynchronizowane w celu wyeliminowania wielu nakładających się rekordów i poprawy dokładności danych. Takie skonsolidowane podejście pozwoliłoby na większą przejrzystość, np. własności nieruchomości, bez potrzeby tworzenia dodatkowych rejestrów.

Doktorantka proponuje także wykorzystanie możliwości oferowanych przez duże zbiory danych. Podaje jako przykład niemieckie systemy rejestracji i wskazuje podmioty prawne, które odgrywają kluczową rolę w walce z praniem pieniędzy i finansowaniem terroryzmu. Według Jej opinii konieczna jest poprawa dokładności danych dotyczących beneficjentów rzeczywistych poprzez reformy metodologiczne rejestru przejrzystości, w połączeniu z rygorystyczną strategią egzekwowania prawa i przy wsparciu odpowiedniego połączenia potencjału ludzkiego i technicznego. Złożony krajobraz podmiotów, zwłaszcza tych z powiązaniami zagranicznymi, stanowi istotne zagrożenie. Przeciwdziałanie mu wymaga głębszego zrozumienia ich roli i podatności na pranie pieniędzy i finansowanie terroryzmu. Opierając się na sektorowych ocenach ryzyka, danych empirycznych i spostrzeżeniach wielu agencji, można uzyskać głębsze zrozumienie, które ułatwia wykrywanie i łagodzenie potencjalnych zagrożeń.

Doktorantka podkreśla problemy obecnych rozwiązań prawnych, które nie wspierają walki z terroryzmem. Instrumenty finansowe na okaziciela, z ich unikalnymi profilami ryzyka, wymagają zastosowania specjalnych środków prawnych w przyszłości. Doktorantka przyjmuje stanowisko, iż oprócz środków legislacyjnych, takich jak zakaz posiadania takich udziałów, w potrzebna jest szersza zmiana kulturowa w kierunku przejrzystości i odpowiedzialności. Przejście na akcje imienne i ustanowienie wzmocnionych mechanizmów egzekwowania prawa może mieć kluczowe znaczenie dla ograniczenia potencjalnych nadużyć.

Niezwykle ciekawym przykładem jest wykorzystanie przez Niemcy zautomatyzowanego systemu odzyskiwania kont, z naciskiem na zapewnienie bezpośredniego dostępu do jednostki analityki finansowej. Zdaniem Doktorantki to strategiczny krok w walce z praniem pieniędzy i finansowaniem terroryzmu. Jednak, jak zaznacza, jego skuteczne wykorzystanie wymaga wdrożenia solidnych środków cyberbezpieczeństwa w celu ochrony integralności danych. Stałe szkolenie, rozwój kompetencji cyfrowych są również niezbędne do zapewnienia umiejętnego korzystania z technologii wsparcia. Moim zdaniem, to najciekawszy wątek poruszany w pracy. W tym kontekście szczególne znaczenie mają przestępstwa związane z tożsamością cyfrową. Problem ten odnosi się do strategii manipulacyjnej polegającej na tworzeniu fikcyjnej tożsamości przy użyciu różnych rodzajów danych osobowych w celu

uzyskania nielegalnych korzyści finansowych lub osobistych. Połączone podstawowe elementy danych osobowych, takie jak imię i nazwisko, data urodzenia i dokumenty identyfikacyjne wydawane przez rząd, są zwykle jednoznacznie powiązane z daną osobą. Ponadto, dodatkowe elementy danych osobowych, takie jak adresy zamieszkania, adresy poczty elektronicznej (e-mail) lub numery telefonów, choć nie są unikalnymi identyfikatorami, wzmacniają postrzeganą legalność fałszywej tożsamości. Aby nielegalnie uzyskać informacje umożliwiające identyfikację osoby, przestępcy stosują różne taktyki. Obejmują one dystrybucję złośliwego oprogramowania za pośrednictwem zwodniczych reklam w mediach społecznościowych, wiadomości phishingowych lub naruszeń danych, a zagrożone dane są często dostępne do sprzedaży w Internecie lub Darknecie. Dlatego też oszustwa związane z syntetyczną tożsamością stają się złożonym przestępstwem, które nie wykorzystuje tożsamość prawdziwej osoby, ale łączy prawdziwe i sfabrykowane dane w celu stworzenia nowej tożsamości. Następnie ta syntetyczna osoba ubiega się o konta bankowe lub karty kredytowe, dokonuje nieuczciwych zakupów i uzyskuje anonimowy dostęp do systemu finansowego, do którego normalnie nie miałyby wstępu. To jednak tylko jeden z wielu przykładów, które wspierają działania terrorystyczne i przestępstwa finansowe. Ciągłe innowacje w technologiach płatniczych, takich jak aplikacje mobilne, znacznie zwiększyły wydajność transakcji. Włączenie wirtualnych aktywów, takich jak kryptowaluty, stanowi kolejny przykład tej ewolucji. Jednak powszechne stosowanie metod kryptograficznych i cyfrowych sprawia, że śledzenie transakcji w tych systemach jest niezwykle złożone, jeśli nie niemożliwe. W procesie przenoszenia środków wirtualne aktywa mogą być kupowane, a następnie przekazywane pośrednikom lub docelowym odbiorcom. Śledzenie przepływu środków staje się coraz trudniejsze w przypadku korzystania z wirtualnych aktywów w porównaniu z tradycyjnymi transakcjami bankowymi. Ponadto nie jest możliwe ustalenie, czy zgłoszone nieprawidłowości mają związek przyczynowy z zakupionymi lub sprzedanymi aktywami wirtualnymi. Wirtualne aktywa są następnie przekazywane docelowym odbiorcom apeli fundraisingowych i ewentualnie sprzedawane. Ze względu na zaciemnione przepływy transakcji często trudno jest określić źródło lub cel funduszy otrzymanych przez odbiorców. Można sobie wyobrazić, że zakupione wirtualne aktywa mogą być wysyłane bezpośrednio do odpowiednich organizacji terrorystycznych i wykorzystywane przez nie do finansowania terroryzmu lub pośrednio do wypłaty środków.

Doktorantka odwołuje się do zmian z 2020 r. w systemie niemieckim, kiedy wprowadzono procedury licencjonowania dla firm zajmujących się przechowywaniem aktywów wirtualnych (dostawców portfeli). W rezultacie firmy zajmujące się

przechowywaniem aktywów wirtualnych wymagają zatwierdzenia przez odpowiednie organy regulacyjne.

W erze cyfrowej postęp technologiczny oferuje transformacyjne rozwiązania. Jego wykorzystanie, zwłaszcza w zarządzaniu danymi i ich wyszukiwaniu, może usprawnić operacje, wyeliminować nadmiarowość i zwiększyć dokładność danych. W szczególności potencjał sztucznej inteligencji lub machine learning w oparciu o duże zbiorów danych może stanowić nowe podejście, dodając bezprecedensową szansę na analityczne podejście do tematu ścigania cyberprzestępczości, wzmacniając tym samym determinację w walce z praniem pieniędzy i finansowaniem terroryzmu. Warto dodać, że w środowisku regulacyjnym Unii Europejskiej pojawiają się propozycje dotyczące wzmocnienia weryfikacji tożsamości cyfrowej, dotyczą one także rynku niemieckiego. Współpraca międzynarodowa koncentruje się także na nowych regulacjach wdrażanych w państwach członkowskich UE, jak również poprzez ramy regionalne, nie poprzestając na regulacjach dotyczących wyłącznie europejskiego nakazu dochodzeniowego lub europejskiego nakazu aresztowania. Spójrzeć należy na takie kierunki regulacyjne, jak: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), a w szczególności Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

Wysoki stopień wzajemnych powiązań między usługami finansowymi, znacząca działalność transgraniczna podmiotów finansowych oraz silne uzależnienie całego sektora finansowego od zewnętrznych dostawców usług ICT wymaga zapewnienia silnej operacyjnej odporności cyfrowej będącej przedmiotem wspólnego zainteresowania w celu zachowania niezawodności unijnych rynków finansowych. Działania unijne są tu konieczne, aby ułatwić wzajemne uznawanie wyników zaawansowanych testów operacyjnej odporności cyfrowej dotyczących podmiotów prowadzących działalność transgraniczną, które w przypadku braku unijnych przepisów podlegają lub mogą podlegać różnym regulacjom w różnych państwach członkowskich. Unijne działania są również konieczne, aby zwalczyć brak odpowiednich uprawnień nadzorczych umożliwiających monitorowanie ryzyka związanego z zewnętrznymi dostawcami usług ICT, w tym ryzyka koncentracji i wystąpienia efektu domina w odniesieniu do unijnego sektora finansowego. Europejska Rada ds. Ryzyka Systemowego (ERRS) potwierdziła, że istniejący wysoki poziom wzajemnych powiązań między podmiotami

finansowymi, rynkami finansowymi i infrastrukturami rynku finansowego, a w szczególności wzajemne zależności między ich systemami ICT mogą potencjalnie stanowić słabą stronę o charakterze systemowym. Poważne konsekwencje cyberataków nasilają się, gdy dochodzi do nich w sektorze finansowym, który jest obszarem o wiele bardziej narażonym na to, że stanie się celem złośliwych ataków dążących do osiągnięcia zysków finansowych bezpośrednio u źródła. Aby ograniczyć takie ryzyko i zapobiec niedostępności lub utracie integralności systemów ICT oraz naruszeniu poufnych danych lub uszkodzeniu fizycznej infrastruktury ICT, należy znacznie usprawnić procedurę zgłaszania przez podmioty finansowe poważnych incydentów związanych z ICT. W konsekwencji, działania dotyczące wspólnych - na jednolitym rynku cyfrowym - rozwiązań dotyczących zabezpieczenia systemów stanowią główny cel obecnej aktywności regulacyjnej w zwalczaniu cyberprzestępczości, co warto było wyraźnie podkreślić w rozprawie.

Doktorantka słusznie podkreśla w podsumowaniu, iż w kontekście zmian należy rozważyć wprowadzenie innowacyjnych technologii. Sztuczna inteligencja i uczenie maszynowe mają potencjał w zakresie predykcyjnego nadzoru policyjnego, wykrywania oszustw i analizy sieci, co znacznie usprawniłoby obecne praktyki w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Takie technologie mogłyby zautomatyzować analizę dużych zbiorów danych, szybciej identyfikować podejrzane wzorce i pomóc śledczym skoncentrować wysiłki na sprawach wysokiego ryzyka. Należy jednak ustanowić silny nadzór i jasne wytyczne, aby zapewnić etyczne wykorzystanie, chronić prawo do prywatności i zapobiegać dyskryminującym praktykom. Co więcej, integracja nowych technologii, w szczególności sztucznej inteligencji, może zwiększyć możliwości analityczne jednostek analityki finansowej poprzez skanowanie dużych ilości danych finansowych i identyfikowanie ukrytych wzorców i anomalii, które mogą wymykać się tradycyjnym technikom analitycznym. Zdolność ta może zmienić krajobraz operacji związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu, zapewniając im bezprecedensową szybkość i dokładność.

Innym interesującym wątkiem jest kwestia aktywności organizacji charytatywnych, które mają zróżnicowany charakter, ale łączy je wspólna misja poprawy warunków społecznych. Organizacje te są często wsparciem dla zmarginalizowanych społeczności, obrony praw człowieka i świadczenia podstawowych usług. Często działają one w strefach wysokiego ryzyka i trudnych środowiskach, w których nawet interwencja rządu może być ograniczona. Pomimo powszechnego potępienia terroryzmu, organizacje te nie są odporne na wykorzystywanie do nielegalnych działań. Takie wykorzystywanie może podważyć zaufanie publiczne do organizacji charytatywnych, choć wpływ ten nie jest równomiernie rozłożony w

całym sektorze. Pozytywny profil publiczny organizacji charytatywnych, poleganie na dobrowolnym wsparciu, różnorodność i szeroki zasięg sprawiają, że są one podatne na nadużycia. Ich działalność na obszarach podatnych na konflikty lub w regionach o słabej infrastrukturze, w połączeniu ze złożonymi transakcjami finansowymi i szerokim zakresem programów, zwiększa tę podatność. Ponadto organizacje pozarządowe lub non-profit mogą mieć nieregularne i nieprzewidywalne przepływy finansowe, co utrudnia identyfikację podejrzanych transakcji. Mogą również prowadzić oddziały lub projekty, które nie są bezpośrednio nadzorowane lub konsekwentnie monitorowane, a także podlegać różnym stopniom regulacji na całym świecie. Co więcej, często służą one jako skuteczne narzędzia do mobilizowania osób wokół wspólnego celu i zbiorowej inicjatywy, nieumyślnie zapewniając istniejące wcześniej wsparcie społeczne i platformę uwiarygodnienia dla osób szerzących terroryzm lub ideologie ekstremistyczne.

Do nadużyć może dojść poprzez częściowe przekierowanie otrzymanych funduszy charytatywnych do grup terrorystycznych lub poprzez nieuczciwe organizacje kontrolowane przez te grupy, które kierują wszystkie fundusze na wspieranie działalności terrorystycznej. W szczególności, niektóre organizacje charytatywne są celem grup terrorystycznych w celu wykorzystania ich zasobów, funduszy i sieci za pomocą różnych metod, w tym przekierowania darowizn, a nawet manipulacji władzami organizacji. Problematyka ta ma ogromny potencjał poznawczy, także w kontekście cyberprzestępczości. Uważam, że może stanowić początek kolejnych, poszerzonych badań Doktorantki.

Należy zauważyć, że przedstawiona do oceny rozprawa nie jest kolejną próbą wypracowania generalnego rozwiązania kwestii przestępczości finansowej jako takiej. Chociaż w pracy wielokrotnie zostało podkreślone znaczenie regulacji – zwłaszcza w tak interesującej części odnoszącej się do kwestii uwarunkowań prawnych w Niemczech, to istotne znaczenie ma pewien konflikt wartości, o którym tylko sporadycznie Doktorantka wspomina, opisując amerykańską ustawę USA PATRIOT Act, która kryminalizuje pranie pieniędzy, zwiększa sankcje cywilne i karne za pranie pieniędzy oraz wzmacnia procedury identyfikacji klientów. Ustawa rozszerza również odpowiedzialność na wszystkie instytucje finansowe i wymaga od nich wdrożenia procedur należytej staranności. Wzmocnione procedury mają zastosowanie do zagranicznych rachunków korespondenckich i prywatnych rachunków bankowych, a instytucje finansowe mają zakaz prowadzenia interesów z zagranicznymi bankami fasadowymi. Ponadto ułatwiono dostęp do rejestrów, a banki są zobowiązane do udzielenia odpowiedzi na rządowe wnioski o udzielenie informacji w ciągu 120 godzin. Podczas rozpatrywania wniosków o połączenia biznesowe, takie jak fuzje lub przejęcia banków, agencje regulacyjne muszą brać

pod uwagę historię banku w zakresie przeciwdziałania praniu pieniędzy. Doktorantka przytacza uwarunkowania geopolityczne wskazując, iż ataki terrorystyczne z 11 września 2001 r. ogólnie sprzyjały większej akceptacji lub uzasadnieniu możliwych stosunkowo daleko idących ograniczeń praw jednostki wynikających ze środków zwalczania terroryzmu i innych działań terrorystycznych, takich jak rozszerzenie uprawnień rządu. Podkreśla, iż w literaturze przedmiotu wskazywano na problem naruszania praw jednostki przez USA. PATRIOT Act była krytykowana, ze względu na uprawnienia śledcze, które mogą również zmniejszyć ogólną skuteczność dążenia do zapewnienia bezpieczeństwa. W 2004 r. sąd federalny orzekł, że części ustawy USA PATRIOT Act dotyczące zobowiązań podmiotów prywatnych do dostarczania danych są niezgodne z konstytucją i prawem do prywatności. Idąc tym tropem Doktorantka podejmuje wyzwanie, iż pozytywnym aspektem jest to, że ustawa USA PATRIOT Act zapewniła organom bezpieczeństwa wewnętrznego, organom ścigania i wywiadowi narzędzia, wytyczne i zasoby do zapobiegania przestępstwom. Nie udziela jednak odpowiedzi na pytania dotyczące granic stosowania tych instrumentów, chociaż taka próba byłaby ciekawym elementem prowadzonej analizy. Rozważania tu przytaczane dotyczą kluczowej kwestii praw podstawowych człowieka i bezpieczeństwa oraz porządku publicznego. Obszar tematyczny rozprawy wpisuje się w ten dyskurs naukowy i jednocześnie moralny oraz uzasadnia charakter przeprowadzonego wywodu w rozprawie i wybraną przez Doktorantkę metodę badawczą.

Przeprowadzona w rozprawie analiza pokazuje ogromne zaangażowanie badawcze Doktorantki i wnikliwe spojrzenie na wybrane zagadnienia poddane analizie. W podsumowaniu pracy Doktorantka dokonała zestawienia w oparciu o własne badania. Podsumowanie odnoszące się do kwestii potrzeby wskazania wybranych regulacji i wyznaczenia kierunków rozwojowych, gdzie wykazano związek ograniczeń z zadaniami określonych podmiotów, którego to rozszerzenia regulacji nie można odnaleźć na gruncie krajowego systemu prawnego, to zabieg niezwykle właściwy. Podobnie jak zastosowanie metody z zarządzania, która może stanowić podstawę do systemowego podejścia do regulacji tego obszaru, jednak z pewnymi kierunkami rozwojowymi dotyczącymi sieci teleinformatycznych. Otóż wydaje się, że brakuje tu bezpośredniego odniesienia do systemowego ujęcia kwestii związanych z samą infrastrukturą krytyczną, jednak zamysł Doktorantki jest mimo to czytelny.

Bardzo trudny i ciekawy temat omówiony został dostatecznie i z dużym wyczuciem poruszanej problematyki. Obszernie i wyczerpująco Autorka zwraca uwagę na trudności związane z odpowiednimi regulacjami, nie pomija także stanowiska zajmowanego przez przytaczaną szeroką literaturę. Koncepcja budowy strategicznego partnerstwa, zwłaszcza z dużymi firmami technologicznymi i innowacyjnymi startupami, z wykorzystaniem technologii

chmurowych i analityki opartej na sztucznej inteligencji, po bezpieczne infrastruktury blockchain, czyli z wykorzystaniem tych narzędzi, które przyczyniają się do zagrożeń, stanowi najlepszą rekomendację dla przyszłych strategów bezpieczeństwa. Dodatkowo w podsumowaniu stwierdzono, że oddzielenie prania pieniędzy od przestępstw źródłowych może być jednym ze sposobów na przygotowanie gruntu dla skuteczniejszego egzekwowanie prawa. Słusznie Doktorantka podkreśla, iż oddzielenie to może pozwolić na opracowanie bardziej precyzyjnych narzędzi i mechanizmów wykrywania, jednocześnie wspierając kulturę organów ścigania, która postrzega pranie pieniędzy jako odrębne przestępstwo z własną złożonością i wymaganą wiedzą specjalistyczną.

### ***5. Uwagi końcowe***

Recenzowana praca prawidłowo przedstawia tematykę wybraną przez Doktorantkę. Postawione zadanie badawcze Doktorantka omówiła w sposób satysfakcjonujący na tym poziomie przeprowadzonych badań.

### ***6. Konkluzja***

**Przedstawiona do recenzji praca pani mgr Caroli Bader pt. „Pranie pieniędzy i finansowanie terroryzmu - zadania i obowiązki sektora finansowego w systemie globalnym” spełnia wymogi stawiane rozprawom doktorskim i może stanowić podstawę dalszych etapów postępowania, w celu nadania Doktorantce stopnia doktora nauk prawnych.**

Katarzyna Chałubińska- Jentkiewicz