Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury
Quarterly of the National School of Judiciary and Public Prosecution
Zeszyt 3 (47)/2022

ARTYKUŁY

Uzyskiwanie przez prokuratora – na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu – informacji i danych od instytucji obowiązanych

DOI:10.53024/4.3.47.2022

JACEK SKAŁA[1]

STRESZCZENIE

Artykuł rozpoczyna wyjaśnienie, dlaczego podjęto problem związany z uzyskiwaniem przez prokuratora informacji od instytucji obowiązanych, podkreślając przy tym, że ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu pozwala na gromadzenie dowodów dotyczących innych przestępstw aniżeli tylko wskazanych w art. 165a i art. 299 k.k. Opisano, na czym polega polityka Anti Money Laundering (AML) w działalności wspomnianych instytucji. Następnie scharakteryzowano proces monitorowania klienta i gromadzenia danych w ramach KYC. Sformułowane zostały konkretne pytania, które prokurator możne skierować do określonych instytucji, licząc, że udzielona odpowiedź wskaże na istotne okoliczności dla prowadzonego śledztwa. W kolejnym rozdziale przedstawiono funkcjonowanie modułu płatności, określono, na czym polegają scenariusze transakcyjne i jakich kolejnych wiadomości można żądać od podmiotów wymienionych w art. 2 ust. 1 ustawy. Zwrócono uwagę, jak ważny charakter ma dokument o nazwie „wewnętrzna procedura instytucji obowiązanej", który dotyczy najważniejszych procedur AML/CFT, m.in.: raportowania o podejrzeniu popełnienia przestępstwa, kontroli i audytu, zarządzania danymi i dokumentacją oraz roli zarządu i AML Officer w firmie. Dalsza cześć opracowania, zatytułowana „Rejestr działalności w zakresie walut wirtualnych", dotyczy zasad dokonywania wpisu w rejestrze, jego charakteru oraz gromadzonych w bazie informacji, które mogą być przydatne dla prokuratora. Artykuł kończy się podsumowaniem podjętego tematu.

---

[1] Prokurator Prokuratury Regionalnej w Krakowie, delegowany do Prokuratury Krajowej, ORCID:0000-0003-4128-0670

Słowa kluczowe: dowody, śledztwo, prokurator, pranie pieniędzy, AML/CFT, KYC, transakcja, klient, płatności

1. WPROWADZENIE

Celem niniejszego opracowanie jest pokazanie, jak wiele informacji i danych można uzyskać od instytucji określanych mianem „obowiązane" na gruncie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[2] (dalej: u.p.p.p.). W odbiorze przedstawicieli organów ścigania wspomniana ustawa ma przede wszystkim zapobiegać dwóm konkretnym przestępstwom. Rzeczywiście tak jest, ale niejako przy okazji realizacji głównego celu zawarte w niej regulacje nakładają na wyszczególnione podmioty różnego rodzaju obowiązki związane z gromadzeniem wielu danych i informacji, które będą przydatne w śledztwie dotyczącym nie tylko czynów stypizowanych w art. 165a i art. 299 k.k.[3]. Prokuratorzy nie wykorzystują jednak owych możliwości i zbyt rzadko sięgają do zapisów u.p.p.p., ograniczając się w zasadzie do stosowania instytucji wstrzymywania transakcji i blokowania rachunków. Autor opracowania ma zamiar pokazać, że można częściej korzystać z możliwości, które oferuje omawiany akt prawny w zakresie gromadzenia materiału dowodowego i dokonywania ustaleń faktycznych.

W tekście sięgnięto do rozwiązań ustawowych tworzących tzw. moduł AML. Jest to zbiór przepisów prawa, procedur wewnętrznych, zaplecza sprzętowego i działań faktycznych, tworzących w instytucji obowiązanej politykę AML/CFT[4]. Z punktu widzenia banku, przedsiębiorstwa czy firmy świadczącej usługi płatnicze taka polityka wiąże się z budową pozytywnego wizerunku firmy i dbałością o jej reputację, a także ochroną kadry zarządzającej i pozostałych pracowników przed zarzutami łamania lub nadużycia prawa, wzmacnianiem zaufania do instytucji obowiązanej wśród klientów oraz potencjalnych inwestorów. W najszerszej perspektywie prowadzenie przez podmioty obowiązane działań AML/CFT przyczynia się do stabilności rynku finansowego w Polsce. W art. 2 ust. 1 u.p.p.p. enumeratywnie wyliczono zamknięty zbiór tych instytucji, przy czym od kilku lat obserwuje się tendencję powiększania się tego katalogu. Mowa m.in. o podmiotach tworzących rynek finansowy (bankach, instytucjach płatniczych, firmach inwestycyjnych i pożyczkowych), zakładach ubezpieczeń i pośrednikach ubezpieczeniowych, osobach

---

2 Dz. U. z 2022 r. poz. 593, ze zm.

3 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2022 r. poz. 1138); dalej: k.k.

4 Skrót „AML/CFT" (ang. Anti Money Laundering/Counter Financing of Terrorism) stanowi zbiorcze określenie przepisów i zasad, które muszą stosować instytucje obowiązane w celu zapobiegania praniu pieniędzy oraz finansowaniu terroryzmu.

wykonujących wolne zawody prawnicze, pośrednikach w obrocie nieruchomościami, operatorach pocztowych, przedsiębiorcach w rozumieniu ustawy – Prawo przedsiębiorców[5], uczestnikach obrotu dziełami sztuki, stowarzyszeniach i fundacjach. Nietrudno sobie wyobrazić, jak wielki zasób informacji, danych i dokumentów o dziesiątkach milionów osób posiadają instytucje obowiązane. Prokuratorzy powinni korzystać z tak zgromadzonej wiedzy.

W dużych organizacjach moduł AML jest narzędziem informatycznym, umożliwiającym realizację przez instytucję ustawowych obowiązków dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Jego podstawową funkcję stanowi autentykacja klientów, identyfikacja „podejrzanych" transakcji, a następnie wygenerowanie alertu do obsługi, jeśli zajdą przesłanki, i ewentualne przekazanie stosownego komunikatu do Generalnego Inspektora Informacji Finansowej. Funkcjonalności modułu związane z obszarem AML dotyczą także weryfikacji klientów i oceny ryzyka związanego z dokonywanymi przez nich transakcjami oraz stosowania środków bezpieczeństwa finansowego. Najlepiej jeśli moduł zarządza operacjami w trybie online, co skutkuje identyfikacją „anomalii transakcyjnych" i natychmiastowym wstrzymaniem realizacji podejrzanych zleceń. Jednak duża część instytucji obowiązanych to niewielkie podmioty, sprowadzające się niekiedy do osoby fizycznej prowadzącej jednoosobową działalność gospodarczą w postaci biura nieruchomości, kancelarii prawnej, biura doradztwa podatkowego lub rachunkowego. U nich polityka AML będzie miała zupełnie inny wymiar aniżeli w ogólnopolskiej firmie świadczącej usługi płatnicze czy w międzynarodowym banku. Dlatego warto zaznaczyć, że ustalenia i wnioski poczynione w dalszej części artykułu odnoszą się przede wszystkim do dużych organizacji o rozbudowanej strukturze, dysponujących specjalnymi działami *compliance* i wyznaczonymi osobami do zajmowania się zadaniami AML. Nie zmienia to faktu, że każda instytucja obowiązana, nawet ta najmniejsza, obligatoryjnie zbiera informacje o swoich klientach i prowadzonych transakcjach, a poważne przestępstwa popełniane są niekiedy przez nieuczciwych ludzi, wykorzystujących niewielkie podmioty gospodarcze.

Autor nie zajmował się w publikacji kwestiami proceduralnymi dotyczącymi uzyskiwania przez prokuratora informacji od instytucji obowiązanych poza ustawowymi mechanizmami przewidzianymi do przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu. Szczegółowe opisanie tego zagadnienia wykracza poza ramy niniejszego opracowania, ale generalnie rzecz biorąc, znajdą

---

[5] Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2021 r. poz. 162, ze zm.).

tu zastosowanie przepisy rozdziału 25 Kodeksu postępowania karnego dotyczące żądania wydania i zatrzymania rzeczy z uwzględnieniem ścieżek dostępu do tajemnicy prawnie chronionej (np. bankowej).

2. MONITOROWANIE KLIENTA

Pierwsza, podstawowa zasada skutecznej polityki AML dotyczy identyfikacji przez instytucje obowiązane swoich klientów w momencie nawiązywania z nimi po raz pierwszy stosunków gospodarczych. Wspomniana polityka stanowi wypadkową różnych wektorów, których siła oddziaływania zależy od rodzaju instytucji, profilu jej działalności, ekspozycji na działania niezgodne z prawem i zaakceptowanego „apetytu na ryzyko". Część zasad ma bardziej ogólny charakter, np. nawiązanie relacji z klientem, które następuje dopiero po zweryfikowaniu jego tożsamości. Zawsze należy wtedy ustalić beneficjenta rzeczywistego transakcji. Nie świadczy się usług na rzecz osób anonimowych lub łamiących prawo. Prowadzi się stały monitoring klientów przez cały okres współpracy z nimi, co wymaga posiadania przez instytucję obowiązaną jak największej liczby informacji i danych o osobie i dokonywanych przez nią operacjach w celu potwierdzenia jej wiarygodności. W bardziej zaawansowanych systemach buduje się profil takiego klienta pod względem jego typowego zachowania (sposób logowania się do systemu, rodzaj dokonywanych transakcji, czynniki behawioralne itd.), który stanowi „wzór" do oceny, czy podejmowane przez niego działania w systemach instytucji obowiązanej nie odbiegają od przyjętej normy; stwierdzenie „anormalnej" sytuacji powodowałoby konieczność sprawdzenia określonych zdarzeń pod kątem AML/CFT.

Nawiązując stosunki gospodarcze, instytucja obowiązana dokonuje identyfikacji klienta, która polega przede wszystkim na zebraniu podstawowych informacji określonych w art. 34 u.p.p.p. oraz zweryfikowaniu jego tożsamości, o czym mowa w art. 37 u.p.p.p. Zweryfikowanie polega na potwierdzeniu ustalonych danych identyfikacyjnych na podstawie dokumentu stwierdzającego tożsamość osoby fizycznej (dowód osobisty, paszport lub karta pobytu), dokumentu zawierającego aktualne dane z wyciągu z właściwego rejestru lub innych dokumentów, danych lub informacji pochodzących z wiarygodnego i niezależnego źródła, o ile są dostępne. Instytucje obowiązane po otrzymaniu danych osobowych od swoich (przyszłych) kontrahentów ponownie sprawdzają je we własnych bazach danych oraz rejestrach publicznych, takich jak Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG), Centralny Rejestr Podmiotów – Krajowa Ewidencja Podatników (CRP KEP) czy Powszechny Elektroniczny System Ewidencji Ludności (PESEL). Dodatkowo weryfikowane są osoby zajmujące eksponowane stanowiska

polityczne (tzw. PEP)[6], podobnie jak podmioty, które mogły zostać objęte międzynarodowymi sankcjami Organizacji Narodów Zjednoczonych, Unii Europejskiej lub poszczególnych państw.

OSOBA FIZYCZNA	OSOBA PRAWNA I JEDNOSTKA NIEPOSIADAJĄCA OSOBOWOŚCI PRAWNEJ
• imię i nazwisko • obywatelstwo • państwo urodzenia oraz numer PESEL,a w przypadku osoby nieposiadającej numeru PESEL – data urodzenia • seria i numer dokumentu stwierdzającego tożsamość klienta • adres zamieszkania – w przypadku posiadania tej informacji przez spółkę • nazwa (firma), numer identyfikacji podatkowej NIP oraz adres głównego miejsca wykonywania działalności gospodarczej – w przypadku osoby fizycznej prowadzącej działalność gospodarczą	• nazwa (firma) • forma organizacyjna • adres siedziby lub adres prowadzenia działalności • NIP; w przypadku jego braku – nazwa państwa rejestracji, nazwy właściwego rejestru oraz numeru i daty rejestracji • dane identyfikacyjne osób reprezentujących klienta

1. Dane identyfikacyjne obligatoryjnie odbierane od klienta przez instytucję obowiązaną na podstawie art. 34 u.p.p.p.

Proces uzyskiwania i sprawdzania podstawowych danych o kliencie nazywany jest w skrócie KYC (ang. Know Your Customer) i powinien być prowadzony

[6] W rozporządzeniu Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 27 lipca 2021 r. w sprawie wykazu krajowych stanowisk i funkcji publicznych będących eksponowanymi stanowiskami politycznymi (Dz. U. z 2021 r. poz. 1381), wydanym na podstawie art. 46c u.p.p.p., za PEP uznano m.in. Prokuratora Generalnego, Zastępcę Prokuratora Generalnego i Prokuratora Krajowego; nie są nimi pozostali prokuratorzy powszechnych jednostek prokuratury, podobnie jak nie są nim sędziowie sądów okręgowych i rejonowych.

z zachowaniem najwyższej staranności[7]. Uzyskanie wspomnianej wiedzy wiąże się także z określeniem źródeł pochodzenia majątku, którym dysponuje osoba fizyczna lub prawna w relacjach z instytucją obowiązaną, tak aby nie dopuścić do prania pieniędzy oraz innych działań łamiących prawo. Polityka KYC powinna skupiać się na pełnej identyfikacji nie tylko klientów, lecz także ich beneficjentów rzeczywistych, tj. podmiotów, na rzecz których faktycznie dokonywane są transakcje. Ma to zapobiegać sytuacjom, kiedy podstawione osoby, tzw. słupy, tylko formalnie zawierają umowy lub dokonują innych rozporządzeń na swój własny rachunek, a w rzeczywistości, dysponując cudzym majątkiem, realizują wolę osoby trzeciej.

Oprócz sprawdzenia klienta podczas pierwszego nawiązania relacji art. 34 u.p.p.p. nakłada na instytucje wymienione w art. 2 ust. 1 u.p.p.p. obowiązek bieżącego monitorowania stosunków gospodarczych z klientem, który realizowany jest przez:

1. analizę dokonywanych przez klienta transakcji w ramach stosunków gospodarczych w celu zapewnienia ich zgodności z wiedzą instytucji obowiązanej o kliencie, rodzaju i zakresie prowadzonej przez niego działalności oraz stopniem przypisanego do danej osoby poziomu ryzyka;
2. badanie źródła pochodzenia wartości majątkowych będących w dyspozycji klienta szczególnie w sytuacji, gdy okoliczności mogą świadczyć o realizacji znamion przestępstwa z zaangażowaniem nielegalnych aktywów;
3. zapewnienie, że posiadane dokumenty, dane lub informacje dotyczące stosunków gospodarczych są na bieżąco aktualizowane.

Prokurator, dysponując wiedzą o działaniu modułu KYC, może zwrócić się do instytucji obowiązanej o wydanie informacji obejmującej dane osobowe konkretnej osoby fizycznej lub dane przypisane do osoby prawnej lub innej jednostki organizacyjnej, która korzysta lub korzystała z usług tej instytucji, a także o wydanie jeszcze innych informacji dotyczącej klienta, ponieważ w trakcie trwania stosunków gospodarczych bank, biuro maklerskie, kancelaria prawna czy giełda walut wirtualnych gromadzą szereg danych i dokumentów o osobie fizycznej lub prawnej. W praktyce może chodzić o zestawienia finansowe potwierdzające jej rentowność, deklaracje o źródłach pochodzenia środków lub beneficjentach

[7] Polityka identyfikacji i uwierzytelniania klientów może ulegać modyfikacjom w zależności od sytuacji społecznej i politycznej. Stało się tak w sytuacji intensywnego napływu do Polski setek tysięcy obywateli Ukrainy, którzy m.in. nie posiadają przy sobie dokumentów umożliwiających rejestracje w instytucjach finansowych i korzystanie z ich usług. Dlatego Urząd Komisji Nadzoru Finansowego skierował do Prezesów Zarządów Banków stanowisko dotyczące zapewnienia uchodźcom z Ukrainy usług bankowych dostosowanych do aktualnych warunków poprzez m.in. niezwłoczne wdrożenie przez banki oferty skierowanej do tej grupy uchodźców (https://www.knf.gov.pl/komunikacja/komunikaty?articleId=77364&p_id=18).

rzeczywistych transakcji, informacje o rezydencji podatkowej, zmianach w organach statutowych spółki, fundacji czy stowarzyszenia. Klient pozostaje w stałym kontakcie z podmiotem świadczącym usługi, a więc można zażądać od instytucji obowiązanej dostarczenia informacji o aktualnych, ale także używanych w przeszłości, numerach telefonów, adresach skrzynki e-mail, a nawet komunikatorach.

Prokurator ma prawo zażądać od instytucji obowiązanej udzielenia odpowiedzi na pytanie, czy klient w relacjach handlowych ukrywał prawdziwe dane osobowe, czy posługiwał się rachunkiem (np. płatniczym, bankowym, w spółdzielczej kasie oszczędnościowo-kredytowej, walut wirtualnych) założonym na inną osobę, podawał się za kogoś innego w kontaktach z pracownikami instytucji, przedkładał dokumenty wzbudzające zastrzeżenia co do ich autentyczności lub rzetelności, podał numeru telefonu należącego do innej osoby, odmawiał przedłożenia określonych dokumentów lub podania źródła pochodzenia środków albo w jeszcze inny sposób utrudniał działanie podmiotu gospodarczego. Doświadczenie pokazuje, że instytucje obowiązane nie zgłaszają organom ścigania wszystkich „incydentów", które pojawiły się w ich relacjach z klientem i czasami dopytanie o wspomniane kwestie może okazać się przydatne w śledztwie. Prokurator ma prawo zwrócić się do banku, instytucji kredytowej czy płatniczej o bardziej analityczną formę informacji, np.:

- czy w relacjach z klientem odnotowano „anomalia" transakcyjne w jego zachowaniu; jeśli tak, to kiedy, czym były spowodowane oraz jak obsłużono alert;
- wykonanie dodatkowych czynności weryfikacyjnych i sprawdzających (*enhanced due diligence*) w stosunku do klienta na potrzeby toczącego się śledztwa (np. czy w jego profilu transakcyjnym pojawiały się raje podatkowe, wypłaty znacznych kwot w bankomatach lub kryptobankomatach, dokonywanie operacji z osobami lub jurysdykcjami objętymi sankcjami międzynarodowymi);
- z jakich usług i produktów korzystał klient;
- przedłożenie indywidualnej (obowiązującej oraz historycznej, jeśli ulegała zmianie) oceny ryzyka przypisanego do danego klienta.

Cenne źródło pozyskiwania materiału dowodowego stanowi prowadzona przez instytucję obowiązaną (np. bank lub giełdę kryptowalutową) identyfikacja klienta i weryfikacja jego tożsamości w oparciu na metodzie wideopołączenia. W związku z rozwojem usług świadczonych „na odległość" przy wykorzystaniu Internetu widoczny jest trend obejmowania stosunkami gospodarczymi lub transakcjami

nowych produktów i usług przy wykorzystaniu zdalnych kanałów dystrybucji[8]. Wdrożenie i funkcjonowanie schematu identyfikacji i weryfikacji tożsamości klientów na podstawie zdalnej konferencji, przeprowadzanej ewentualnie przy jednoczesnym wykorzystaniu metod biometrycznych, powoduje, że w bazach instytucji obowiązanych pozostają takie cyfrowe artefakty, jak zapis głosu ludzkiego i wyglądu twarzy (ewentualnie jeszcze innych, indywidualnych cech biometrycznych człowieka), skany dokumentów stwierdzających tożsamość lub inne dokumenty ze zdjęciem (np. prawo jazdy). Gromadzone są także uzupełniające dokumenty potwierdzające tożsamość klienta i adres jego pobytu, np. rachunki za media. Na instytucji obowiązanej ciąży wymóg archiwizowania zapisów wideo (dźwięku i obrazu) z rozmowy z klientami, a w procedurach banku powinny znajdować się odpowiednie przepisy dotyczące nagrywania i przechowywania podobnych treści.

3. MONITORING TRANSAKCJI

Niektóre instytucje obowiązane, w tym przede wszystkim banki, dysponują zaawansowanymi modułami płatności, gdyż w każdej sekundzie obsługują tysiące klientów. W module rejestruje się i przechowuje informacje o wpłatach środków na rachunek bankowy operatora wraz z oznaczeniem klienta, czasu i wysokość wpłaty, danych identyfikujących rachunek i osobę, od której pochodzą aktywa, oraz aktualne saldo na rachunku. Podobnie ewidencjonuje się wypłaty środków. Przekazywane w tym zakresie raporty dla prokuratora powinny obejmować pełne informacje o dokonanych transferach, m.in. poprzez wskazanie numerów rachunków wykorzystanych do przeprowadzenia operacji oznaczone identyfikatorem Międzynarodowego Numeru Rachunku Bankowego (IBAN) lub identyfikatorem zawierającym kod kraju oraz numer rachunku w przypadku rachunków nieoznaczonych IBAN. Tym samym instytucja obowiązana powinna zaniechać przyjmowania przelewów pieniężnych od podmiotów, które udostępniają w ramach operacji mniejszy zakres danych aniżeli podane lub w ogóle ich nie przekazują. Poczyniona uwaga dotyczy realizujących przelewy tzw. szybkich bramek płatności oraz pozostałych aplikacji i produktów zaliczanych do branży FinTech, nierzadko powiązanych z konwersją walut wirtualnych. Narzędzia takie chętnie wykorzystywane są przez przestępców, aby uniemożliwić ustalenie źródła pochodzenia środków, którymi dysponują.

---

[8] W „Rekomendacji D" z 2013 r. dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach Komisja Nadzoru Finansowego dopuściła możliwość potwierdzania tożsamości i uprawnień klientów korzystających z elektronicznych kanałów dostępu, ale przy minimalizacji ryzyka udzielenia dostępu nieupoważnionym osobom (https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf).

Profesjonalny moduł płatności operuje na komputerowych algorytmach nazywanych „scenariuszami". Ich zadanie polega na monitoringu operacji finansowych (offline lub/i online) i wykrywaniu tzw. anomalii transakcyjnych (tj. transakcji odbiegających od przyjętego, pozytywnego wzorca), rejestracji w systemie ujawnionych incydentów i generowaniu alertów do obsługi przez administratora AML łącznie z blokowaniem podejrzanych rachunków.

SCENARIUSZE TRANSAKCYJNE MOGĄ DOTYCZYĆ ZDARZEŃ:
rachunków, na które wpłynęło więcej niż X przelewów, a ich suma przekroczyła Y w określonym przedziale czasu;
przekroczenia sumy wpłat lub/i wypłat w określonym przedziale czasu;
przypadków, jeśli rzeczywiste wpływy w skali miesiąca na rachunki przekroczą wskazaną wielokrotność X i jednocześnie przekroczą łącznie kwotę Y dla wskazanej klasy ryzyka;
przypadków, jeżeli suma wpłat i/lub wypłat klienta przekroczyła wartość Y w określonym przedziale czasu;
raportowania do Głównego Inspektora Informacji Finansowej o wpłacie lub wypłacie środków pieniężnych o określonej wartości.

2. Przykładowe scenariusze transakcyjne stosowane przez instytucje finansowe (opracowanie własne autora)

Historia związana z monitorowaniem transakcji jest przechowywana przez instytucję obowiązaną przez 5 lat. Art. 49 u.p.p.p. stanowi bowiem, że instytucje przechowują – licząc od dnia zakończenia stosunków gospodarczych z klientem lub od dnia przeprowadzenia transakcji okazjonalnej – dowody potwierdzające przeprowadzone transakcje i ewidencje transakcji, obejmujące oryginalne dokumenty lub kopie dokumentów konieczne do identyfikacji operacji. Prokurator ma prawo sięgnąć do tego cennego zasobu informacji w ramach każdego śledztwa, jeśli tylko okaże się, że mogą znajdować się w nim ślady lub dowody popełnionego przestępstwa albo inne dane mające znaczenie dla ustalenia okoliczności faktycznych sprawy.

W trakcie postępowania przygotowawczego może zachodzić konieczność ustalenia, czy instytucja finansowa należycie wdrożyła i stosowała środki bezpieczeństwa finansowego w zakresie przeciwdziałania praniu pieniędzy, a więc czy implementowany przez nią monitoring przepływów środków pieniężnych był efektywny. W przeciwnym razie osoby odpowiedzialne za zaniedbania mogą ponieść

odpowiedzialność karną z art. 156 u.p.p.p., a nawet z art. 299 § 2 k.k., jeśli świadomie ułatwiły „pranie" aktywów pochodzących z przestępstwa. Skorzystanie przez prokuratora z omawianych źródeł dowodowych będzie dotyczyło także ustalenia *modus operandi* sprawców innych czynów zabronionych (np. oszustw internetowych, kradzieży z włamaniem do aplikacji mobilnych bankowości elektronicznej), a pytanie skierowane do podmiotu opisanego w art. 2 ust. 1 u.p.p.p. może być sformułowane w następujący sposób: „Czy w zachowaniu klienta były symptomy mogące świadczyć o prowadzeniu przez niego nielegalnej działalności z wykorzystaniem zasobów i bazy logistycznej instytucji obowiązanej poprzez:

- posługiwanie się wieloma rachunkami zarejestrowanymi na inne osoby;
- wielokrotne przewalutowanie środków zgromadzonych na rachunkach lub konwersji pomiędzy pieniądzem fiducjarnym a walutami wirtualnymi bez sprecyzowanego celu biznesowego;
- korzystanie przez klienta z bankomatów, wpłatomatów, kryptobankomatów lub innych urządzeń umożliwiających anonimowe wpłaty/wypłaty gotówki i walut wirtualnych bez racjonalnego uzasadnienia w profilu transakcyjnym klienta;
- wykorzystywanie do transakcji („wejścia" lub „wyjścia") niestandardowych metod płatności, takich jak: Mistertango, N26, Revolut, Western Union, Wirex, PayPal, MoneyGram;
- anulowanie przez klienta zlecenia transakcji w momencie powzięcia wiadomości, że zaszły przesłanki do jej raportowania do GIIF.

Osobna kwestia dotyczy kontaktów „na odległość". Napisano już, że charakteryzuje je większy poziom ryzyka aniżeli zlecenie realizowane tradycyjnymi źródłami komunikowania się (tj. „przy okienku" w banku, podczas umówionego spotkania z doradcą finansowym czy w punkcie obsługi klienta). Z treści art. 76 u.p.p.p. wynika, że na instytucji obowiązanej ciąży ustawowy nakaz posiadania informacji lub dokumentów dotyczących m.in. adresów IP, z których następowało połączenie klienta z systemem teleinformatycznym instytucji obowiązanej oraz znaczników czasu połączeń z systemem. Zgromadzenie przez prokuratora historii logów być może pozwoli ustalić wiele istotnych danych o osobie pozostającej w jego zainteresowaniu, np. geolokalizację urządzeń elektronicznych, z których korzystała, oraz częstotliwość i czas/okres jej kontaktów z instytucją obowiązaną. Dodatkowa analiza adresów IP w świetle zgromadzonego materiału dowodowego może udowodnić, że:

1. transakcje realizowano z IP uprzednio wykorzystanych do nielegalnych działań (np. oszustw, ataków phishingowych, dystrybucji złośliwego oprogramowania typu ransomware);

2. transakcje dokonywano z krajów objętych sankcjami, rajów podatkowym lub z innego „egzotycznego" terytorium;
3. osoba pozostająca w zainteresowaniu organów ścigania używała narzędzi anonimizujących ruch sieciowy (TOR, VPN-y, proxy);
4. zachodzą rozbieżności między adresami IP powiązanymi z profilem klienta a tymi, z których inicjowano transakcje (można z tego wnioskować, że osoba objęta śledztwem była „słupem", a jej dane osobowe wykorzystał beneficjent rzeczywisty transakcji).

Przykładowy, ogólny schemat spożytkowania informacji uzyskanych od instytucji obowiązanej mógłby wyglądać następująco: w dostarczonej prokuratorowi opinii biegły napisał, że w zbadanej przez niego pamięci dowodowego komputera ujawnił ślady połączeń nawiązywanych z internetową giełdą kryptowalutową (tj. podmiotem, o którym mowa w art. 2 ust. 1 pkt 12 u.p.p.p.). W złożonych zeznaniach świadek zaprzeczył jednak, aby posiadał wiedzę o funkcjonowaniu tokenów cyfrowych i korzystał z nich. W celu zweryfikowania treści zeznań prokurator zwrócił się do giełdy o udzielenie informacji na temat połączeń realizowanych z adresu IP dedykowanego zabezpieczonemu komputerowi z giełdą w okresie ostatnich 5 lat oraz przedstawienie aktywności transakcyjnej osoby, która za pomocą ustalonego IP dokonywała połączeń. Na podstawie informacji zwrotnej potwierdzono, że świadek łączył się z giełdą, posługując się danymi osobowymi tzw. słupa, zlecał liczne wymiany bezgotówkowego pieniądza bankowego na bitcoiny, które następnie przesyłał na ustalony adres portfela. Analiza rachunku bankowego, który użytkował na giełdzie, doprowadziła prokuratora do banku i okazało się, że wpływające do niego środki pochodziły z ataków hakerskich na konta klientów wspomnianego wcześniej banku połączone z kradzieżą zgromadzonych na rachunkach środków. Opisane kluczowe ustalenia zdecydowały o wydaniu postanowienia o przedstawieniu zarzutów i ogłoszenia go podejrzanemu.

4. WEWNĘTRZNE PROCEDURY AML/CFT

Czynności instytucji obowiązanej związane z monitorowaniem klientów i transakcji muszą być szczegółowo opisane w wewnętrznej procedurze w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, określonej przez ustawodawcę mianem „wewnętrznej procedury instytucji obowiązanej" (art. 50 ust. 1 u.p.p.p.). Stanowi ona najważniejszy dokument w firmie, jeśli chodzi o realizację zadań wyznaczonych ustawą AML, i prokurator powinien zażądać od instytucji jego wydania wraz z załącznikami (np. formularzem identyfikacji klienta), jeśli prowadzi śledztwo związane z podmiotem określonym w art. 2 ust. 1 u.p.p.p. W art. 50 ust. 2 pkt. 1-11 u.p.p.p. wyliczono, co obejmują w szczególności

zasady postępowania. Oprócz kontroli osób i przepływów finansowych wewnętrzna procedura zgodności dotyczy następujących kwestii:

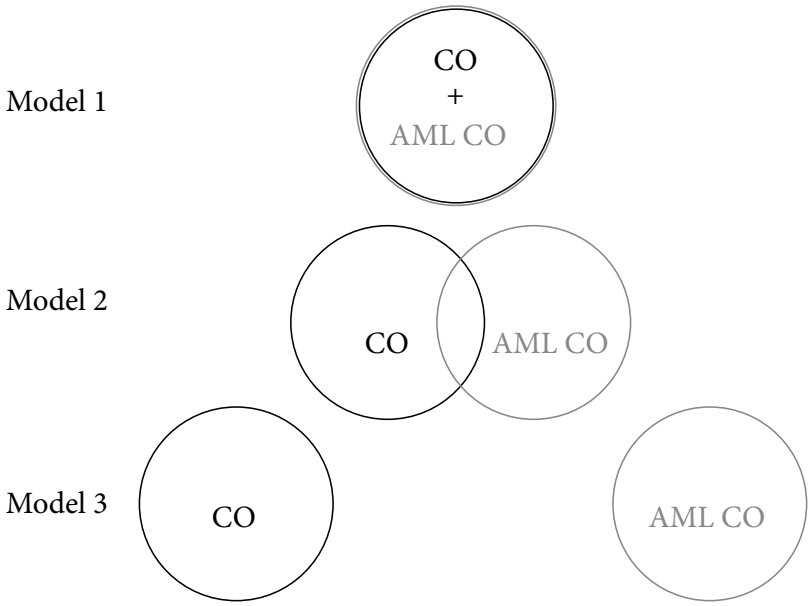
1. „Poznaj swojego pracownika" (ang. Know Your Employee KYE);
2. „Poznaj oferowany produkt" (ang. Know Your Product KYP);
3. wewnętrzne raportowanie o podejrzeniu AML/CFT;
4. zewnętrzne raportowanie o podejrzeniu AML/CFT;
5. zarządzanie danymi i dokumentacją;
6. realizacja „Programu szkoleń";
7. kontrola i audyt;
8. strukturalny podział zadań i kompetencji w zakresie przeciwdziałania AML/CFT pomiędzy Zarządem, Kierownikiem AML, Zespołem AML i ogółem pracowników zatrudnionych w instytucji.

Wymienione procedury mogą być zapisane w jednym dokumencie lub stanowić kilka odrębnych zbiorów poświęconych określonej tematyce. Ustawodawca wymaga, aby znajdujące się w nich zapisy były aktualne, podlegały bieżącej weryfikacji w razie zmiany stosunków, a ponadto uwzględniały charakter, rodzaj i rozmiar prowadzonej działalności przez instytucję obowiązaną. Analiza wspomnianego dokumentu (lub dokumentów) powinna dostarczyć kluczowych informacji dla śledztwa, dotyczących m.in.: metodyki ustalania, rejestrowania i raportowania do GIIF transakcji „podejrzanych", zasad identyfikacji i autentykacji klienta, gromadzenia informacji o konsumentach oraz analizy danych pod kątem oceny poziomu ryzyka przypisanego konkretnej osobie fizycznej lub prawnej.

Z dokumentu opisanego w art. 50 ust. 1 u.p.p.p. prokurator dowie się, jakie procedury wewnętrzne posiada instytucja obowiązana, czego one dotyczą, w jakiej formie i gdzie są przechowywane zapisy je ustanawiające. Już na samym wstępie może się okazać, że nie sporządzono wymaganych przez prawo dokumentów, co skutkuje odpowiedzialnością nie tylko administracyjną, lecz także karną konkretnych osób fizycznych lub prawnych. Po wstępnych ustaleniach można podjąć czynności procesowe w kierunku zabezpieczenia repozytoriów na potrzeby postępowania karnego. W zasadzie każdy z tych dokumentów może okazać się przydatny w zależności od zakresu podmiotowego i przedmiotowego prowadzonego śledztwa.

Na podstawie „wewnętrznej procedury" ustala się przykładowo osoby odpowiedzialne w instytucji za realizację polityki przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, a w szczególności, czy zostali wyznaczeni pracownik zajmujący kierownicze stanowisko, odpowiedzialny za wykonanie obowiązków ustawowych AML/CFT, (art. 8 u.p.p.p.) oraz nadzorująca go kadra kierownicza wyższego szczebla (art. 7 u.p.p.p.). Zebranie takich informacji jest kluczowe dla przypisania indywidualnej odpowiedzialności karnej za popełnienie przestępstwa

z art. 156 u.p.p.p. W praktyce jednak ustalenie takich okoliczności bywa skomplikowane, bowiem zadania AML Officera i Compliance Officer nachodzą na siebie i w rezultacie odpowiedzialność konkretnych osób często „rozmywa się". Instytucje obowiązane o charakterze korporacyjnym ustanawiają różne modele podziału kompetencji związanych z zapewnieniem zgodności działalności instytucji i dyspozycji art. 8 u.p.p.p.; może wykonywać je łącznie jedna osoba, niekiedy obowiązki Compliance Officer i AML Officer krzyżują się, a w trzecim rozwiązaniu są ściśle rozgraniczone pomiędzy dwa podmioty.



3. Modele relacji pomiędzy Compliance Officer i AML Officer (opracowanie własne autora)

Analiza procedury „Poznaj swojego pracownika" (KYE) dostarczy informacji na temat pracowników instytucji obowiązanej (byłych i obecnych). W zbiorze można odnaleźć CV (życiorys zawodowy) danej osoby z wyszczególnieniem jej danych, poprzednich miejsc pracy i zajmowanych stanowisk, okresu ich sprawowania, świadczenia innych usług na podstawie umów cywilnoprawnych związanych z rynkiem finansowym, przedłożoną przez kandydata informację z Krajowego Rejestru Karnego. Ponadto sprawdzić można, czy dokumenty potwierdzają kompetencje pracownika do jego zatrudnienia na sprawowanym stanowisku. Korporacje monitorują osoby w okresie ich zatrudnienia pod kątem realizacji powierzonych im zadań oraz identyfikują i zgłaszają Zarządowi wszelkie nieprawidłowości w tym zakresie, które mogą być uznane za sprzeczne z polityką AML/CFT. Dla prokuratora ów *research* stanowi trudne do przecenienia źródło wiedzy o świadku

lub podejrzanym i przypomina nieco „wywiad środowiskowy", ale przeprowadzony w świecie finansów.

5. REJESTR DZIAŁALNOŚCI W ZAKRESIE WALUT WIRTUALNYCH

Instytucja obowiązana, wykonująca czynności opisane w art. 2 ust. 1 pkt 12 u.p.p.p., prowadzi działalność regulowaną w rozumieniu prawa przedsiębiorców i ma obowiązek uzyskania wpisu do rejestru działalności gospodarczej w zakresie walut wirtualnych. Wynika to z art. 129m u.p.p.p., który został wprowadzony ustawą z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw[9] (obowiązuje od października 2021 r.). Jak wskazano w uzasadnieniu projektu, wprowadzenie omawianych przepisów wynika z obowiązku nałożonego na Polskę i pozostałe państwa członkowskie UE na mocy dyrektywy AML V mówiącej, aby podmioty świadczące usługi wymiany walut pomiędzy walutami wirtualnymi a fiducjarnymi podlegały przymusowi uzyskania stosownej rejestracji. Ustawa precyzuje ponadto, kto może wykonywać wspomnianą działalność, co powinien zawierać wpis, jakie dane gromadzone są w rejestrze i kiedy następuje wykreślenie podmiotu z bazy elektronicznej. Dane w rejestrze są przechowywane przez okres 5 lat, licząc od dnia, w którym dokonano wykreślenia podmiotu z rejestru działalności w zakresie walut wirtualnych (art. 129y u.p.p.p.).

Organem właściwym w sprawach rejestru jest Minister Finansów, ale faktycznie prowadzi go Izba Administracji Skarbowej w Katowicach. Według stanu na dzień 8 kwietnia 2022 r. w rejestrze widniało 161 podmiotów; część z nich to osoby fizyczne, ale większość działała w charakterze spółek prawa handlowego. Przedsiębiorcy deklarowali świadczenie różnego rodzaju usług związanych z rynkiem „krypto"; najczęściej chodziło o wymianę pomiędzy walutami wirtualnymi i środkami płatniczymi, a także pomiędzy samymi walutami wirtualnymi, pośrednictwo we wskazanych wymianach oraz prowadzenie rachunków płatniczych w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[10]. Z otwartych źródeł internetowych wynika, że zarejestrowane firmy oferowały usługi finansowe polegające na kupnie, sprzedaży, wymianie i przechowywaniu wielu rodzajów kryptowalut, takich jak: bitcoin, ethereum, ripple czy dogecoin; niektóre działały w branży IT i oprogramowania komputerowego, inne prowadziły lombardy lub zarządzały kryptobankomatami.

---

[9] Dz. U. z 2021 r. poz. 815.

[10] Dz. U. z 2021 r. poz. 1907, ze zm.

Rejestr stanowi bardzo cenne źródło wiedzy dla prokuratora, zwłaszcza że wiele platform cyfrowych zajmujących się kryptowalutami działa w „podejrzanych" jurysdykcjach i kontakt z nimi, bezpośrednio lub w ramach międzynarodowej pomocy prawnej, jest znacznie utrudniony, a nawet niemożliwy. Tymczasem podmiot wnioskujący o wpis do rejestru zobowiązany jest podać następujące dane: imię i nazwisko albo nazwę (firmę) przedsiębiorcy, numer w rejestrze przedsiębiorców lub w Krajowym Rejestrze Sądowym, o ile taki numer został nadany oraz NIP, a ponadto określić rodzaj świadczonych usług w zakresie walut wirtualnych, o których mowa w art. 2 ust. 1 pkt 12 u.p.p.p. Dzięki temu prokurator uzyskuje cenne informacje: na jaki adres należy wysyłać decyzje lub inne pisma procesowe skierowane do instytucji obowiązanej, jak kształtuje się skład właścicielski, zarząd i reprezentacja danej spółki oraz jakie usługi świadczy podmiot pozostający w jego zainteresowaniu. Informacje uzyskane od Dyrektora Izby Administracji Skarbowej w Katowicach mogą stanowić punkt wyjścia do dalszych ustaleń oraz gromadzenia dokumentów i danych z innych urzędów publicznych (np. właściwego urzędu skarbowego, Zakładu Ubezpieczeń Społecznych) o osobie fizycznej lub prawnej pozostającej w zainteresowaniu organów ścigania.

Oprócz informacji przekazanych we wniosku o wpis, rejestr działalności w zakresie walut wirtualnych zawiera ponadto: numer i datę wpisu oraz informacje o zakończeniu takiej działalności przez dany podmiot. Dochodzą do tego zgłoszenia i dokumenty zgromadzone w procesie rejestracji lub później. Chodzi m.in. o wymóg przedłożenia przez osoby fizyczne zaświadczeń o ukończeniu szkolenia lub kursu obejmujących prawne lub praktyczne zagadnienia związane z działalnością w zakresie walut wirtualnych lub wykonywania, przez okres co najmniej roku, podobnej aktywności zawodowej, potwierdzonych odpowiednimi dokumentami, poświadczających posiadaną wiedzę lub doświadczenie na rynku „krypto". Uzyskanie takich informacji nierzadko ma kluczowe znaczenie przy ocenie zawinienia danej osoby lub jego braku oraz ewentualnie formy tego zawinienia (umyślność lub nieumyślność). Co więcej, chociaż wpis ma posiadać charakter deklaratoryjny, to w pewnych przypadkach Minister Finansów będzie uprawniony do przeprowadzenia postępowania administracyjnego i dokonania daleko idących ustaleń faktycznych. Z art. 129s pkt 2 u.p.p.p. wynika, że organ właściwy w sprawach rejestru odmówi, w drodze decyzji, dokonania wpisu, jeżeli dane zawarte we wniosku są niezgodne ze stanem faktycznym. To oznacza, że właściwy minister będzie zobowiązany do ustalenia okoliczności sprawy, a następnie wydania decyzji, która ma wpływ na sytuację prawną i faktyczną podmiotu wykonującego działalność w zakresie walut wirtualnych. Z kolei art. 129w ust. 3 pkt a i b u.p.p.p. stanowi, że organ właściwy w sprawach rejestru działalności w zakresie walut wirtualnych

wykreśla, w drodze decyzji, podmiot wykonujący taką działalność z elektronicznej bazy w przypadku stwierdzenia:

1. niespełniania przez podmiot warunków wymaganych prawem do wykonywania działalności w zakresie walut wirtualnych;
2. że podmiot złożył oświadczenie, o którym mowa w art. 129r ust. 2 u.p.p.p., niezgodne ze stanem faktycznym.

Słusznie zauważa W. Srokosz[11], że takie uprawnienia organu publicznego noszą znamiona działań nadzorczych. Jeśli w przypadku przedsiębiorcy mogą one wiązać się z koniecznością wykonania dodatkowych czynności i przedłożenia określonych dokumentów, to dzięki temu powstanie bogaty zbiór danych, które prokurator będzie mógł wykorzystać przy dokonywaniu ustaleń: kto prowadził działalność związaną z walutami wirtualnymi, w jakim okresie, jakie były powiązania osobowe i kapitałowe podmiotu wpisanego do rejestru, gdzie mieściła się siedziba firmy, jaki był (deklarowany) poziom wiedzy i doświadczenie osoby nią zarządzającej, jakim posługiwała się numerem telefonu lub adresem skrzynki e-mail (kontrola operacyjna). Organ prowadzący rejestr może dysponować ponadto dokumentacją związaną z kondycją finansową przedsiębiorców wpisanych do bazy czy innymi pochodzącymi od nich rekordami. W chwili obecnej, gdy waluty wirtualne stały się nieodłącznym elementem wielu przestępstw, baza danych ustanowiona na podstawie art. 129m u.p.p.p. może okazać się trudnym do przecenienia rezerwuarem informacji do efektywnego wykorzystania w niejednym śledztwie.

6. PODSUMOWANIE

Umiejętność skutecznego poszukiwania śladów i dowodów popełnionego przestępstwa, ich prawidłowe kryminalistyczne i procesowe zabezpieczanie, a następnie skuteczne wykorzystanie w procesie to jedna z najważniejszych cech pracy kompetentnego prokuratora. Dlatego w śledztwie, zwłaszcza skomplikowanym, nie należy ograniczać się do utartych środków i źródeł pozyskiwania materiału dowodowego, ale warto być kreatywnym i podjąć wysiłek ustalenia stanu faktycznego sprawy wykorzystując różnego rodzaju informacje i dane. Jedną z dróg osiągnięcia tego celu, szczególnie w sprawach przeciwko mieniu, stanowi sięgnięcie do baz danych instytucji obowiązanych, opisanych w ustawie z dnia 1 kwietnia 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. W artykule pokazano, jak wiele cennych wiadomości gromadzą i przetwarzają wskazane podmioty. Gdyby dobrze się zastanowić, to takich „niekonwencjonalnych" źródeł dowodowych

[11] Zob. W. Srokosz, *Technologia rozproszonego rejestru (DLT) na rynku finansowym z uwzględnieniem wybranych zagadnień prawnych*, „Monitor Prawa Bankowego" 2021, nr 6, s. 49.

jest więcej. Stosunkowo rzadko w trakcie śledztwa korzysta się z możliwości, jakie daje ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi[12]. Stanowi ona, że prokurator – za pośrednictwem Krajowego Biura do spraw Odzyskiwania Mienia – może zwrócić się do wielu podmiotów z zapytaniem o składniki majątkowe posiadane przez określoną osobę poza granicami Polski, jej rachunku bankowego, pojazdy, którymi dysponuje, udziały w podmiotach gospodarczych, informacje podatkowe czy dotyczące tej osoby notowania kryminalne. Jest to procedura uzyskiwania informacji o wiele szybsza w realizacji aniżeli złożenie wniosku w ramach międzynarodowej pomocy prawnej i warto z niej skorzystać przed podjęciem oficjalnych działań w ramach europejskiego nakazu dochodzeniowego lub systemu MLAT. Wszystko po to, aby bezbłędnie ustalić stan faktyczny sprawy oraz winę lub brak zawinienia konkretnej osoby na podstawie – parafrazując paremię łacińską – „dowodów jaśniejszych od światła" (łac. *In criminalibus probationes debent esse luce clariores*).

BIBLIOGRAFIA

Literatura

Srokosz W., *Technologia rozproszonego rejestru (DLT) na rynku finansowym z uwzględnieniem wybranych zagadnień prawnych*, „Monitor Prawa Bankowego" 2021, nr 6.

Akty prawne

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2021 r. poz. 2345, ze zm.).
Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2021 r. poz. 1907, ze zm.).
Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz. U. z 2020 r. poz. 158, ze zm.).
Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593, ze zm.).
Ustawa z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2021 r. poz. 162, ze zm.).
Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (Dz. U. z 2021r. poz. 815).
Rozporządzenie Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 27 lipca 2021 r. w sprawie wykazu krajowych stanowisk i funkcji publicznych będących eksponowanymi stanowiskami politycznymi (Dz. U. z 2021 r. poz. 1381).
Komunikat dot. stanowiska Komisji Nadzoru Finansowego z dnia 4 marca 2022 r. w sprawie usług bankowych dla uchodźców z Ukrainy, https://www.knf.gov.pl/komunikacja/komunikaty?articleId=77364&p_id=18.

[12] Dz. U. z 2020 r. poz. 158, ze zm.

Rekomendacja D Komisji Nadzoru Finansowego ze stycznia 2013 r., dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf.

Tabele i wykresy

Obtaining information and data by the prosecutor from obligated institutions under the Act of March 1, 2018 on counteracting money laundering and financing of terrorism

SUMMARY

The article begins with an explanation of why the problem of gaining information by prosecutor from the obliged institutions was addressed. It has also been highlighted that the bill of 1 March 2018 contraposing money laundering and finansing terrorism also allows gathering evidence referring to other crimes than the ones described in art 165a p.c. and art. 299 p.c. The policy of Anti Money Laundering in the above mentioned institutions was then explained. The process of customer monitoring and KYC data gathering was then characterised. The author has formulated specific questions which a prosecutor can put forward to a financial institution, hoping that the answer they receive will indicate crucial circumstances for the investigation. In the next part, the article describes functioning of payment module, the functioning of transactional scenarios and what other information one can require from the entities mentioned in art. 2 act 1 of the bill. Special attention has been put to the importance of the document called 'inner procedure of the obliged institution', which refers to the most important procedures AML/CFT, committing crime suspicion report, control and audit, data management and the role of the board and AML Officer in a company amongst others. The next part of the text entitled 'virtual currency activities record pertains to the rules of signing up in the record, its character and the information gathered in the set which can be useful for a prosecutor. The article concludes with a summary of the topic undertaken.

Key words: evidence, investigation, prosecutor, money laundering, AML/CFT, KYC, transaction, client, payments