https://doi.org/10.4467/27204383TER.23.018.18320

https://orcid.org/0000-0002-4015-5774
https://orcid.org/0000-0002-2761-3144
https://orcid.org/0009-0000-7130-0455

PAWEŁ OPITEK
AGNIESZKA BUTOR-KELER
KAROL KANCLERZ

Wybrane aspekty przestępczości z wykorzystaniem walut wirtualnych

Abstrakt

Artykuł składa się z dwóch części. W pierwszej omówiono zagadnienia związane z funkcjonowaniem rynku kryptoaktywów w Polsce i na świecie oraz planowanymi zmianami w przepisach regulujących ten rynek. Dotyczą one statusu prawnego tokenów cyfrowych i ich wykorzystania w procederze prania pieniędzy i finansowania terroryzmu oraz obowiązków instytucji obowiązanych w systemie przeciwdziałania praniu pieniędzy. W drugiej części skupiono się na kwestiach procesowych i pozaprocesowych związanych z kryptowalutami. Omówiono status cyfrowego artefaktu w postępowaniu karnym, pracę operacyjną oraz prowadzenie śledztwa pod kątem zwalczania przestępczości kryptowalutowej. W podsumowaniu przedstawiono postulaty skierowane do organów ścigania i ochrony prawa. Celem artykułu jest przegląd problematyki dotyczącej wykorzystania walut wirtualnych w popełnianiu przestępstw, zwłaszcza zagadnień z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Słowa kluczowe:

kryptowaluty,
waluty wirtualne,
przestępczość,
pranie pieniędzy,
finansowanie terroryzmu,
śledztwo,
ślady i dowody cyfrowe

Waluty wirtualne stały się nieodłącznym elementem popełniania różnego rodzaju przestępstw – stanowią one przedmiot czynności wykonawczej, gdy sprawca pozbywa osobę uprawnioną władztwa nad bitcoinami, a statuujące je dane binarne stają się obiektem nieuprawnionych manipulacji. Nierzadko kryptowaluty są wykorzystywane do prania pieniędzy, uzyskiwania okupu za ataki oparte na socjotechnice lub oprogramowaniu typu ransomware. Dochodzi także do malwersacji finansowych z wykorzystaniem kryptowalut i crowdfundingu, platform działających podobnie jak tradycyjny rynek Forex czy piramid finansowych, których klienci są kuszeni obietnicą szybkiego i wysokiego zysku po zainwestowaniu w tokeny. Są również emitowane kryptoaktywa stanowiące de facto pochodne instrumenty finansowe z ominięciem przepisów regulujących funkcjonowanie rynku kapitałowego. Zjawisko kryptowalut jest analizowane nie tylko w kontekście modus operandi sprawców czynów zabronionych. Wiążą się z nim także inne ważne zagadnienia, takie jak: status prawny tokenów, analiza kryminalna transferów kryptowalutowych, tymczasowe zajęcie mienia ruchomego i zabezpieczenie majątkowe na bitcoinie lub innych altcoinach, procedury uzyskiwania śladów cyfrowych i międzynarodowa pomoc prawna w tym zakresie czy administracyjne procedury AML/CFT (ang. *Anti-Money Laundering/Counter Financing of Terrorism*). Niniejszy artykuł stanowi ujęcie tych wszystkich zagadnień, jednak z uwagi na jego ograniczoną objętość tylko niektóre z nich mogły zostać omówione bardziej szczegółowo.

Na wstępie warto zadać pytanie: czy polskim organom ścigania przestępstw w ogóle są potrzebne zdolności dotyczące pracy z kryptoaktywami? Odpowiedź na tak postawione pytanie jest z całą pewnością twierdząca, co wynika z kilku powodów. Najogólniej rzecz biorąc, współczesny obraz przestępczości zbyt często jest powiązany z walutami wirtualnymi i technologią tworzącą system rozproszonych rejestrów, aby formacje przeznaczone do ochrony ekonomicznych interesów państwa nie orientowały się w prawnych, ekonomicznych i technicznych aspektach ich funkcjonowania. Ale są też konkretne sprawy, które zobowiązują np. Agencję Bezpieczeństwa Wewnętrznego do zainteresowania się kryptowalutami. Służą one do prania pieniędzy na dużą skalę, a ABW jest zobligowana do rozpoznawania i wykrywania przestępstw godzących w podstawy ekonomiczne państwa oraz zapobiegania im. Bezpieczeństwo to także przestrzeganie przez Polskę zawartych umów międzynarodowych, gdyż ma to bezpośredni wpływ na jej pozycję i renomę na arenie światowej. W tym kontekście warto przypomnieć, że sankcje nałożone na Rosję i Białoruś po agresji Federacji

Rosyjskiej na Ukrainę obejmują także kryptoaktywa i polskie służby nie mogą dopuścić do tego, aby te sankcje były omijane z wykorzystaniem krajowych dostarczycieli usług sieciowych. Anonimowe transfery na blockchainie mogą również stanowić dogodne narzędzie do wspierania organizacji terrorystycznych i agentury wpływu istniejącej w różnych państwach, także w Polsce. Agencja Bezpieczeństwa Wewnętrznego ma za zadanie kontrolować ten segment szeroko pojętego rynku finansowego w celu zapobiegania takim działaniom.

Artykuł opiera się na dwóch celach badawczych: analizie aktualnego statusu prawnego i faktycznej funkcjonalności kryptoaktywów na świecie oraz ustaleniu, czy wiążą się one i na jaką skalę z popełnianiem czynów zabronionych, w tym z praniem pieniędzy oraz finansowaniem terroryzmu. W tym drugim przypadku, oprócz krytycznego spojrzenia na międzynarodowy wymiar omawianej przestępczości, podjęto także bliski autorom opracowania temat działań organów ścigania w zakresie walki z przestępczością kryptowalutową. Analiza omawianej przestępczości w skali mikro (krajowej) i makro (globalnej) doprowadziła do wskazania działań, które wymagają od organów ścigania wiedzy na temat kryptowalut i wykorzystania jej w praktyce.

Zastosowana metodologia badań polegała na obserwacji oraz analizie różnorodnych źródeł internetowych związanych z walutami wirtualnymi i ustaleniu sposobów funkcjonowania tych walut oraz na przemyśleniach autorów artykułu na temat rozpatrywanych zagadnień. Autorzy zapoznali się m.in. z informacjami zawartymi na stronach specjalistycznych firm z branży krypto oraz organizacji rządowych, w tym z raportem z przeprowadzonego w Kongresie Stanów Zjednoczonych wysłuchania przedstawicieli służb walczących z terroryzmem poświęconego aktywności ekstremistów w świecie wirtualnym. Ponadto autorzy – na podstawie własnych kompetencji i doświadczeń zawodowych zdobytych w ramach zajmowania się sprawami karnymi czy też realizacji zadań nadzorczych nad rynkiem kapitałowym – przedstawili wnioski na temat przestępczości kryptowalutowej i działalności polskich służb w tym zakresie. Skonfrontowano je z materiałami źródłowymi w postaci analiz, raportów oraz innych opracowań organizacji i instytucji zajmujących się cyfrowymi tokenami i technologią blockchain. Odwołano się także do obowiązujących lub będących w fazie projektowania aktów prawnych regulujących rynek krypto. Finalnie, na podstawie całości uzyskanych informacji, zastosowano metodę

indukcyjną polegającą na zapisaniu spostrzeżeń poczynionych w odniesieniu do stwierdzonego wcześniej zbioru danych.

W artykule określenia: kryptowaluty, waluty wirtualne i kryptoaktywa (aktywa cyfrowe) są używane zamiennie, gdyż dotyczy on przestępczości i ta dowolność terminologiczna nie ma większego znaczenia dla opisu tematu badań. Należy jednak podkreślić, że określeniem o najszerszym zakresie pojęciowym są kryptoaktywa, chociaż w prawie polskim brakuje ich definicji legalnej. Według *Rozporządzenia wykonawczego Prezydenta Stanów Zjednoczonych z dnia 9 marca 2022 r. w sprawie zapewnienia odpowiedzialnego rozwoju zasobów cyfrowych*[1] pojęcie aktywów cyfrowych odnosi się do pieniędzy cyfrowych emitowanych przez bank centralny (ang. *central bank digital currency*, CBDC) niezależnie od zastosowanej technologii ich emisji oraz do innych reprezentacji wartości, w tym papierów wartościowych, pochodnych instrumentów finansowych oraz innych produktów finansowych, które są wykorzystywane do dokonywania płatności, inwestowania, przesyłania lub wymiany funduszy lub ich ekwiwalentu, emitowane lub reprezentowane w formie cyfrowej przy użyciu technologii rozproszonej księgi rozrachunkowej (ang. *distributed ledger technology*, DLT) niezależnie od nazwy produktu. Pojęcie kryptowalut dotyczy natomiast aktywów cyfrowych, które mogą być środkiem wymiany, generowanych lub obsługiwanych przez technologię DLT. Pośrodku zakresów pojęciowych tych dwóch określeń lokują się waluty wirtualne.

Status prawny tokenów cyfrowych

Waluty wirtualne są różnie traktowane na świecie pod względem regulacji prawnych. Mimo że w niektórych państwach uznano je za prawny środek płatniczy, to są to sytuacje wyjątkowe, gdyż najczęściej odmawia się im pozycji podobnej do tej, jaką ma pieniądz fiducjarny. Wynika to z tego, że rządy poszczególnych państw rygorystycznie strzegą swojego monopolu na emisję pieniądza, gdyż dzięki niemu mogą kształtować politykę monetarną kraju i wpływać na procesy gospodarcze. Badania przeprowadzone przez Międzynarodowy Fundusz Walutowy pokazują, że najmocniejszą pozycję

[1] *Ensuring Responsible Development of Digital Assets*, Executive Order 14067 of March 9, 2022, Federal Register. The Daily Journal of the United States Government, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [dostęp: 5 IV 2023]. Tłumaczenia w artykule pochodzą od autorów (dop. red.).

waluty wirtualne zyskały w Afryce Subsaharyjskiej, gdzie 25% krajów szczegółowo uregulowało ich status prawny, a ponad połowa z nich zdecydowała się na zniesienie wielu ograniczeń dotyczących funkcjonowania kryptowalut na tradycyjnym rynku finansowym[2]. Dotyczy to jednak regulacji w zakresie tokenów płatniczych, takich jak bitcoin, a więc najprostszych w swoim działaniu. Na przykład w październiku 2021 r. Bank Centralny Nigerii wprowadził wirtualnego tokena o nazwie eNaira jako wsparcie dla tradycyjnego pieniądza fiducjarnego. System opracowała firma Fintech Bitt, a dwie aplikacje do korzystania z eNairy – eNaira Speed Wallet i eNaira Merchant Wallet – są dostępne w sklepach z aplikacjami Google i Apple. W 2022 r. wyemitowano już 500 mln eNair (1,21 mln dolarów), ale nigeryjski rząd jednocześnie zakazał dokonywania transakcji we własnym sektorze bankowym innymi kryptowalutami[3].

W krajach wysoko rozwiniętych podejmuje się natomiast inicjatywy mające na celu usystematyzowanie podejścia do zaawansowanych tokenów cyfrowych emitowanych na podstawie technologii blockchain i podobnych w działaniu do pochodnych instrumentów finansowych. Prace nad tokenizacją takich instrumentów są bardzo zaawansowane w Japonii. W październiku 2021 r. MUFG, największy japoński bank, ogłosił wyniki prac grupy Security Token Research Consortium (przemianowanej w 2022 r. na Digital Asset Co-creation Consortium) zajmującej się budową infrastruktury dla tokenizowanych papierów wartościowych. Zaplanowano ewidencjonowanie obrotu nimi na blockchainie korporacyjnym Corda. Prawo podłączenia się do niego przyznano innym firmom zainteresowanym cyfrowymi instrumentami finansowymi – papierami wartościowymi notowanymi na giełdzie Osaka Digital Exchange, która zintegrowała się z platformą Progmat i umożliwia dokonywanie transakcji P2P (ang. *peer-to-peer*)[4] pomiędzy inwestorami[5]. Platforma cały czas poszerza swoją funkcjonalność

[2] *Living on the Edge*, International Monetary Fund, październik 2022 r., https://www.imf.org/en/Publications/REO/SSA/Issues/2022/10/14/regional-economic-outlook-for-sub-saharan-africa-october-2022 [dostęp: 5 IV 2023].

[3] P. Opitek, *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain*, Łódź 2022, s. 214.

[4] Transakcje P2P – transakcje dokonywane między osobami fizycznymi z wyłączeniem pośredników, np. sklepów, oraz fabryk i korporacji (przyp. red.).

[5] *MUFG, SBI share roadmap for Japanese security tokens*, Ledger Insights, 7 X 2021 r., https://www.ledgerinsights.com/mufg-sbi-share-roadmap-for-japanese-security-token-platform/ [dostęp: 27 III 2023].

(rozrosła się z 80 firm do 163 pod koniec 2022 r.) i obecnie kładzie nacisk na rozwój i obrót stablecoinem, umożliwiającym dokonywanie rozliczeń poza oficjalnym systemem bankowym[6].

Po drugiej stronie plasują się państwa, które całkowicie zakazały posiadania walut wirtualnych, tj. Chiny, Nepal, Bangladesz, Afganistan, Maroko, Algieria i Boliwia[7]. W przypadku Państwa Środka istnieje kilka powodów, dlaczego tak się stało. Chiny mają kilkuletnią przewagę nad resztą rozwiniętych gospodarek globu w rozwoju narodowej waluty cyfrowej Banku Centralnego, a więc tamtejszy rząd mógł postrzegać zdecentralizowane aktywa jako konkurencję zagrażającą projektowi scentralizowanego juana. Ponadto ustrój ekonomiczny Chin preferuje odgórne zarządzanie rynkiem finansowym i zapewne istnienie autonomicznego bitcoina nie jest dla niego korzystne. W rezultacie chińskie władze zaczęły prowadzić politykę antykryptowalutową i medialne akcje marketingowe odradzające korzystanie z bitcoinów i altcoinów. Ostatecznie wprowadzono zakaz wyszukiwania w Internecie haseł związanych z kryptowalutami, jak również zamykanie cyfrowych platform[8].

W Stanach Zjednoczonych oraz w państwach Unii Europejskiej posiadanie walut wirtualnych jest dozwolone, a jedyne obowiązki z tym związane dotyczą jakieś formy rejestracji (zgłoszenia) działalności gospodarczej prowadzonej z wykorzystaniem kryptowalut. Problematyczna jest emisja instrumentów finansowych na blockchainowych protokołach. W Europie takie działania są zasadniczo zabronione, a w Stanach Zjednoczonych obowiązuje zasada neutralności technologicznej i można tokenizować instrumenty finansowe, chociaż w praktyce jest to obwarowane koniecznością spełnienia wielu wymogów i generalnie nieopłacalne. Niedawno Biały Dom opublikował pierwszy raz w historii wytyczne w celu kompleksowego określenia ram odpowiedzialnego rozwoju zasobów cyfrowych w Stanach Zjednoczonych. Zgodnie z zarządzeniem prezydenta Joe Bidena administracja tego kraju sformułowała zalecenia dotyczące ochrony konsumentów, inwestorów, przedsiębiorstw, stabilności finansowej, bezpieczeństwa

---

[6] *MUFG's Progmat security token platform to become digital asset joint venture,* Ledger Insights, 22 XII 2022 r., https://www.ledgerinsights.com/mufg-progmat-security-token-digital-asset-joint-venture/ [dostęp: 5 IV 2023].

[7] F. O'Sullivan, *Where Is Crypto Illegal in 2023? The Countries That Ban Cryptocurrency,* Cloudwards, 22 II 2023 r., https://www.cloudwards.net/where-is-crypto-illegal/ [dostęp: 5 IV 2023].

[8] P. Opitek, *Funkcjonowanie instrumentów finansowych…*, s. 212.

narodowego i środowiska w kontekście funkcjonowania rynku krypto. Rozporządzenie wykonawcze z 9 marca 2022 r. w sprawie zapewnienia odpowiedzialnego rozwoju zasobów cyfrowych[9] nakreśliło nowatorskie podejście do przeciwdziałania zagrożeniom oraz wykorzystania potencjalnych korzyści płynących z zasobów cyfrowych i leżącej u ich podstaw technologii. Agencje rządowe opracowały ramy i zalecenia wspierające m.in. ochronę konsumentów i inwestorów, promowanie stabilności finansowej i konkurencyjności gospodarczej oraz innowacyjności. Stany Zjednoczone są uznawane także za światowego lidera w stosowaniu procedur przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu w środowisku zasobów cyfrowych i ustanawiają w tej sferze globalne standardy. Biały Dom zaznaczył, że popularność kryptoaktywów spowodowała także wzrost liczby cyberprzestępców dokonujących m.in. prania pieniędzy oraz finansowania nielegalnej działalności. W celu przeciwdziałania takim praktykom konieczne są: zwiększenie zakresu regulacji dotyczących rynku kryptowalut i nadzoru nad nim, intensywniejsze zaangażowanie organów ścigania w walkę z omawianą przestępczością oraz zmiana przepisów prawa, w tym najważniejszej amerykańskiej ustawy o tajemnicy bankowej (ang. *The Bank Secrecy Act*, BSA), zaostrzenie kar przewidzianych za anonimowe przesyłanie wartości majątkowych w formie krypto oraz sprawienie, aby dotyczyły one także dostawców usług związanych z giełdami internetowymi i niewymienialnych NFT (ang. *non-fungible token* – niepowtarzalne tokeny utożsamiające zdigitalizowane dzieło sztuki, np. rzeźbę lub obraz malarski). W ramach podjętych działań Biały Dom zobowiązał Departament Sprawiedliwości USA do ścigania poważnych przestępstw związanych z aktywami cyfrowymi dokonywanych w dowolnej jurysdykcji, a Ministerstwo Skarbu do finalizacji w 2023 r. oceny ryzyka nielegalnego finansowania zdecentralizowanych finansów[10].

W UE z kolei brakuje – zdaniem Komisji Europejskiej – jednolitych przepisów mających zastosowanie do usług związanych z kryptoaktywami, co naraża konsumentów i inwestorów instytucjonalnych na znaczne ryzyko strat. Ponadto fakt, że niektóre państwa członkowskie wprowadziły na szczeblu krajowym stosowne regulacje, a inne tego nie zrobiły, prowadzi

[9] *Ensuring Responsible Development*...

[10] *White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets*, The White House, 16 IX 2022 r., https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ [dostęp: 9 IV 2023].

do fragmentacji wspólnego prawa, która zakłóca konkurencję na jednolitym europejskim rynku, utrudnia usługodawcom rozszerzanie ich działalności na skalę transgraniczną i prowadzi do arbitrażu regulacyjnego. Dlatego Parlament Europejski wkrótce przegłosuje przyjęcie rozporządzenia w sprawie rynków kryptaktywów (ang. *Markets in Crypto-assets*, MiCA). Rozporządzenie ustanowiłoby zharmonizowane na szczeblu UE przepisy dotyczące takich wartości majątkowych, zapewniając w ten sposób pewność prawa w odniesieniu do kryptoaktywów nieobjętych obowiązującym prawodawstwem unijnym. Ma to zwiększyć ochronę konsumentów i inwestorów oraz stabilność finansową, promować innowacje i możliwości wykorzystania tokenów opartych na technologii DLT. Rozporządzenie ustanawia trzy rodzaje kryptoaktywów: tokeny powiązane z aktywami (przypominające stablecoiny), tokeny pieniądza elektronicznego oraz kryptoaktywa nieobjęte prawodawstwem UE. Już we wstępnym porozumieniu negocjacyjnym ustalono bardzo istotne kwestie, takie jak chociażby zabezpieczenie płynności i wykupu kryptoaktywów w taki sposób, aby były one zabezpieczone wartością walut referencyjnych (reguła 1:1). Emitent kryptoaktywów będzie zobowiązany zapewnić ich wykup w razie zawirowań na rynku. Ma to na celu zapewnienie wysokiego poziomu ochrony konsumentów i inwestorów oraz integralności ekosystemu krypto, a także minimalizację zagrożeń dla stabilności finansowej i polityki pieniężnej, które mogą wyniknąć z szerokiego wykorzystania kryptoaktywów i technologii DLT w praktyce[11].

Parlament Europejski pracuje także nad nowym rozporządzeniem mającym na celu zaostrzenie polityki dotyczącej walut wirtualnych przez zlikwidowanie luki regulacyjnej. Zaostrzenie to ma polegać na zobowiązaniu zdecentralizowanych organizacji typu DAO[12], platform NFT i DeFi[13]

---

[11] *Proposal for a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [dostęp: 9 IV 2023]; *Markets in crypto-assets (MiCA)*, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221 [dostęp: 9 IV 2023].

[12] DAO (ang. *decentralized autonomous organization*) – zdecentralizowana organizacja, która podejmuje autonomiczne decyzje zarządcze zgodnie z wolą posiadaczy tokenów *governance*, czyli takich, które dają prawo głosowania.

[13] DeFi (ang. *decentralized finance*) – zdecentralizowany system finansowy zaprojektowany dla nieograniczonej liczby inwestorów, przeznaczonych dla nich blockchainowych platform, produktów i usług finansowych oraz ich twórców. DeFi korzysta na różne sposoby z pieniądza fiducjarnego, rachunków bankowych czy bezgotówkowych systemów płatności, jednak najważniejsze są kryptowaluty, innowacyjne protokoły rozproszonego rejestru

do przestrzegania przepisów AML na takich samych zasadach, jakie obowiązują tradycyjne podmioty rynku finansowego. W kwietniu 2023 r. Departament Skarbu Stanów Zjednoczonych opublikował pierwszą na świecie kompleksową ocenę ryzyka związanego z nielegalnym finansowaniem DeFi. Wynika z niej, że przestępcy chętnie wykorzystują usługi rynku „zdecentralizowanych finansów", przede wszystkim do czerpania korzyści z ataków ransomware, kradzieży, oszustw, handlu narkotykami i finansowania proliferacji, a także działań wspierających terroryzm. Najważniejsze czynniki ułatwiające im takie działania wynikają z nieobowiązywania w DeFi procedur AML/CFT i KYC[14], małego stopnia cyberbezpieczeństwa protokołów oraz tego, że ich administratorzy działają często w jurysdykcjach nierespektujących mechanizmów międzynarodowej pomocy prawnej lub w ogóle nie sposób ich powiązać z jakimkolwiek terytorium[15]. Planuje się zatem zobowiązać instytucje kredytowe i finansowe do stosowania wyśrubowanych reguł należytej staranności przy realizacji transakcji krypto o wartości przekraczającej 1000 euro, a relacje biznesowe z komercyjnymi podmiotami nielicencjonowanymi byłyby całkowicie zabronione. Taki sam limit, tj. 1000 euro, dotyczyłby przelewów pochodzących z portfeli hostowanych samodzielnie, kiedy ustalenie personaliów posiadacza takiego portfela jest znacznie utrudnione. Władze UE zaproponowały również ustanowienie nowego organu ds. przeciwdziałania praniu pieniędzy, który będzie nadzorował i egzekwował przepisy AML we wszystkich 27 krajach UE[16].

---

i inteligentne umowy (ang. *smart contracts*) przypominające konta bankowe i lokaty, różne formy kredytów oraz finansowe instrumenty pochodne. Klienci indywidualni oraz instytucjonalni dostarczają kapitał dla funkcjonowania DeFi i oczekują zysku z poczynionych inwestycji, tym bardziej że oferowana stopa zarobku jest często znacznie wyższa niż na tradycyjnym rynku kapitałowym. Z drugiej strony inwestowanie w DeFi wiąże się ze stosunkowo dużym ryzykiem utraty zaangażowanych środków lub brakiem korzyści obiecanych przez tradera. Decentralizacja DeFi oznacza, że nie ma jednej wiodącej organizacji czy instytucji, która odpowiada za cały system bądź jego poszczególne elementy. Zob. P. Opitek, *Funkcjonowanie instrumentów finansowych*..., s. 156.

[14] KYC (ang. *Know Your Customer*) – procedura należytej staranności, którą instytucje finansowe oraz inne prawnie określone podmioty muszą przeprowadzać w celu zidentyfikowania swoich klientów (przyp. red.).

[15] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. Department of the Treasury, kwiecień 2023 r., https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [dostęp: 14 IV 2023].

[16] I. Preiss, *Crypto AML rules passed by MEPs*, The Block, 28 III 2023 r., https://www.theblock.co/post/223215/crypto-aml-rules-passed-meps [dostęp: 6 IV 2023].

W polskim prawie jedyna definicja legalna dotycząca tokenów cyfrowych zakotwiczonych w blockchainie znajduje się w *Ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (dalej: u.p.p.p.). Zbudowana jest ona z dwóch elementów: mówi, czym waluta wirtualna nie jest (np. prawnym środkiem płatniczym), oraz wymienia jej pozytywne cechy, takie jak: cyfrowe odwzorowanie wartości, wymienialność w obrocie gospodarczym na prawne środki płatnicze, akceptowalność jako środka wymiany, możliwość elektronicznego przechowywania lub przeniesienia albo możliwość bycia przedmiotem handlu elektronicznego. Chociaż szczegółowa analiza prawna tej definicji[17] wykracza poza ramy niniejszego artykułu, to należy zaznaczyć, że w praktyce jej wykładnia oraz stosowanie sprawia wiele trudności. Nie ulega wątpliwości, że dotyczy ona bitcoina i pozostałych altcoinów, ale można odnieść wrażenie, że organy nadzoru nad rynkiem finansowym nie potrafią jednoznacznie odnieść się do pytania, czy art. 2 ust. 2 pkt 26 u.p.p.p. dotyczy także stablecoinów lub tokenów NFT. Można zaryzykować tezę, że polski ustawodawca nie zamierza podjąć samodzielnych działań w kierunku ściślejszego uregulowania rynku krypto, tylko czeka na zmiany procedowane w Parlamencie Europejskim. Jest to po części uzasadnione tym, że wspólna europejska polityka dotycząca kryptoaktywów jest kształtowana na poziomie unijnym i nie ma sensu wprowadzać specyficznych rozwiązań krajowych w przeddzień wejścia w życie takich regulacji, jak np. MiCA.

Pranie pieniędzy z wykorzystaniem walut wirtualnych

Przestępstwo prania pieniędzy zostało stypizowane w art. 299 Kodeksu karnego[18] i jako przedmiot ochrony zakłada bezpieczeństwo obrotu gospodarczego oraz legalne pochodzenie wartości majątkowych. Spośród opisanych w tym przepisie przedmiotów czynności wykonawczej, jak np. środki płatnicze, instrumenty finansowe, papiery wartościowe, to waluta wirtualna będzie wchodziła w zakres prawa majątkowego. Pojęcie prawa majątkowego odnosi się bowiem do wszelkich praw, które realizują interes

[17] Taka analiza została przeprowadzona w artykule: G. Ocieczek, P. Opitek, *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Consilium Iuridicum" 2022, nr 3–4, s. 122–139.

[18] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny*.

ekonomiczny uprawnionego i składają się na jego majątek[19]. Jak wynika z *Crypto Crime Report*[20] firmy Chainanalysis, w latach 2017–2022 waluty wirtualne wykorzystano w procederze „prania" na kwotę ponad 33 mld dolarów, a transfer znacznej części owej wartości dokonywał się z wykorzystaniem giełd internetowych. Tylko w 2021 r. ten wolumen wyniósł prawie 9 mld dolarów, z czego ponad 750 mln transferowano na platformy DeFi. Obserwowane trendy wskazują, że platformy zdecentralizowanych finansów stają się coraz popularniejszym środowiskiem do inwestowania nielegalnie uzyskanych środków, a rok 2022 był pod tym względem rekordowy[21]. Rezultatem tego są, wspomniane wcześniej, prace Parlamentu Europejskiego i administracji Stanów Zjednoczonych nad ściślejszym objęciem DeFi regulacjami AML.

Doświadczenie zawodowe autorów artykułu także potwierdza, że waluty wirtualne są wykorzystywane do popełniania różnego rodzaju przestępstw, m.in. handlu narkotykami, przemytu broni, oszustw, uchylania się od płacenia podatków, cyberataków, opłacania działań sabotażowo-dywersyjnych, handlu ludźmi i czynów związanych z wykorzystaniem dzieci na tle seksualnym. Od pewnego czasu postrzega się kryptowaluty jako potencjalne źródło finansowania korupcji, ale badania tego zjawiska miały ogólny charakter i opierały się bardziej na przypuszczeniach niż na przekonującej metodologii[22]. Sprawa Sama Bankmana-Frieda pokazała jednak, że taka przestępczość istnieje. Bankman-Fried został oskarżony przez amerykańskiego prokuratora o zdefraudowanie miliardów dolarów wpłaconych przez oszukanych klientów na rzecz jego firmy o nazwie FTX.com operującej kryptowalutami. W śledztwie ustalono, że chcąc zapewnić sobie przychylność polityków, Bankman-Fried wpłacał milionowe darowizny na kampanie wyborcze zarówno Partii Demokratycznej, jak i Partii Republikańskiej[23]. Ponadto w listopadzie 2021 r. miał wręczyć

[19] *Prawo cywilne – część ogólna*, M. Safjan (red.), seria: System Prawa Prywatnego, t. 1, Warszawa 2007, s. 717.

[20] Chainalysis, *The 2022 Crypto Crime Report*, luty 2022 r.

[21] Tamże.

[22] Zob. M. Alnasaa i in., *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*, International Monetary Fund, 25 III 2022 r., https://www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676 [dostęp: 4 V 2023].

[23] *United States of America v. Samuel Bankman-Fried*, https://storage.courtlistener.com/recap/gov.uscourts.nysd.590940/gov.uscourts.nysd.590940.80.0.pdf [dostęp: 9 IV 2023].

łapówkę w wysokości 40 mln dolarów co najmniej jednemu chińskiemu urzędnikowi w zamian za skłonienie go do odblokowania przez Państwo Środka kryptowalut o wartości miliarda dolarów zajętych przez chińskie organy ochrony prawa[24].

Okazuje się ponadto, że międzynarodowe organizacje przestępcze coraz częściej używają tokenów cyfrowych do przenoszenia i ukrywania zysków z handlu narkotykami. Dotyczy to przede wszystkim krajów Ameryki Łacińskiej, w których nielegalne grupy wykorzystują giełdy działające bez procedur KYC i AML, aby wyprać miliardy dolarów rocznie i tą drogą przenieść część swoich zasobów finansowych do świata wirtualnego w celu uniknięcia wykrycia przez prokuraturę i konfiskaty „owoców przestępstwa". Dotyczy to m.in. meksykańskich karteli Cártel Jalisco Nueva Generación i Sinaloa Cartel, a także Mara Salvatrucha z Ameryki Środkowej oraz Primeiro Comando da Capital z Brazylii. W tych samych obszarach geograficznych rosnąca liczba skorumpowanych rządów specjalnie dereguluje rynek krypto, aby zainwestowane na nim środki uzyskane w wyniku przekupstwa pozostały anonimowe. Takie działania pokrywają się z interesami Rosji, której sojusznicy w Ameryce Południowej, jak np. reżim Maduro w Wenezueli, opracowali własne systemy kryptowalutowe pozwalające uniknąć sankcji nałożonych na Federację Rosyjską przez państwa euroatlantyckie i ominięcie zachodnich rynków walutowych. Wenezuelską kryptowalutę petro wykorzystuje się do transferów wartości między Wenezuelą a Rosją za pośrednictwem rosyjskich banków[25]. Takiej aktywności dotyczył akt oskarżenia wniesiony przez prokuratora w październiku 2022 r. do Sądu Federalnego w Nowym Jorku. Pięciu obywatelom Rosji postawiono w nim zarzuty związane z nielegalnymi zakupami technologii wojskowej dla Federacji Rosyjskiej (m.in. zaawansowanych półprzewodników i mikroprocesorów stosowanych w samolotach myśliwskich, systemach rakietowych i kosmicznych systemach wojskowych), jej przemytu oraz prania pieniędzy z wykorzystaniem kryptowalut. W procederze noszącym znamiona przestępstwa uczestniczyli

[24] M. Sigalos, R. Goswami, *Sam Bankman-Fried paid over $40 million to bribe at least one official in China, DOJ alleges in new indictment*, CNBC, 28 III 2023 r., https://www.cnbc.com/2023/03/28/sam-bankman-fried-paid-over-40-million-to-bribe-at-least-one-chinese-official-doj-alleges-in-new-indictment.html [dostęp: 9 IV 2023].

[25] D. Farah, M. Richardson, *The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America*, Georgetown University, 20 III 2023 r., https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/ [dostęp: 6 IV 2023].

także przedstawiciele Petróleos de Venezuela S.A., wenezuelskiej państwowej firmy naftowej. Złożony schemat przestępczy przewidywał m.in. transfery kryptowalut o wartości milionów dolarów, które posłużyły do zakupów technologii poza oficjalnym rynkiem finansowym, a także „wyprania" wpływów z nielegalnych działań[26]. W tym kontekście można dodać, że 2 marca 2022 r. Prokurator Generalny USA powołał Task Force KleptoCapture jako grupę zadaniową organów ścigania, której zadaniem jest egzekwowanie szeroko zakrojonych sankcji i ograniczeń eksportowych nałożonych na Rosję.

W UE i Stanach Zjednoczonych standardy w zakresie uregulowań o charakterze administracyjnym poświęconych regulacji rynku walut wirtualnych pod kątem przeciwdziałania praniu pieniędzy są kształtowane przez Grupę Specjalną ds. Przeciwdziałania Praniu Pieniędzy (ang. Financial Action Task Force, FATF[27]). W 2021 r. zaktualizowała ona swoje wytyczne dotyczące podejścia opartego na ryzyku w stosunku do obrotu walutami wirtualnymi i usługodawców operujących na tym rynku (ang. Virtual Assets Service Poviders, VASP)[28]. W raporcie FATF pt. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*[29] (wrzesień 2020 r.) wskazano zalety technologiczne kryptoaktywów i blockchaina, ale też zagrożenia, jakie generuje nowa technologia. Nadużyciom sprzyja duża anonimowość transferów, funkcjonowanie serwisów bezpośredniej wymiany wartości typu P2P, „tumblerów" i „mikserów", a także odmienność uregulowań prawnych dotyczących walut wirtualnych istniejących w różnych jurysdykcjach. Samo pojęcie tokena cyfrowego ma bowiem wieloznaczny charakter i poszczególne tokeny mogą różnić się między

[26] *Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme*, United States Attorney's Office, Eastern District of New York, 19 X 2022 r., https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money [dostęp: 7 IV 2023].

[27] Financial Action Task Force została utworzona w 1989 r. przez Międzynarodowy Fundusz Walutowy i obecnie skupia 37 krajów członkowskich. Celem FATF jest definiowanie standardów i promowanie środków prawnych służących do zwalczania prania pieniędzy, finansowania terroryzmu i innych poważnych zagrożeń integralności globalnego systemu finansowego. Chociaż FATF nie decyduje wprost o rozwiązaniach w zakresie AML/CFT przyjętych przez poszczególne kraje, to de facto ma zasadniczy wpływ na ich kształt.

[28] Virtual Asset Service Provider to dostarczyciel platformy wirtualnej i innych usług służących do zarządzania walutami wirtualnymi.

[29] *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, FATF, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html [dostęp: 7 IV 2023].

sobą pod wieloma względami. Przekłada się to na działanie prokuratora, który staje niekiedy przed trudnym zadaniem ustalenia, czym są kryptoaktywa ujawnione w toku śledztwa.

Podkreśla się rolę poszczególnych państw w zwalczaniu omawianej przestępczości oraz wskazuje, w jaki sposób powinny one monitorować zagrożenia i oceniać ryzyko z nimi związane. Walka z praniem pieniędzy na rynku krypto pozostaje przedmiotem stałego zainteresowania UE, a państwa Starego Kontynentu inkorporowały do swojego ustawodawstwa instytucje przeciwdziałające procederowi prania pieniędzy albo są w trakcie wprowadzania nowych rozwiązań. Chodzi m.in. o zasadę *travel rule*, która dotyczy przekazywania i udostępniania informacji o transakcjach przez dostawców usług działających na rynku aktywów wirtualnych. Takie rozwiązanie zwiększa przejrzystość transferów, a więc możliwości ustalenia osób zaangażowanych w operacje i blokowania podejrzanych środków. Wdrożenie *travel rule* ogranicza także ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu, zwłaszcza w odniesieniu do transferów o charakterze międzynarodowym[30]. Kolejny instrument porządkowania rynku krypto dotyczy obowiązku ustanowienia w każdym państwie UE rejestru dla podmiotów prowadzących działalność w zakresie walut wirtualnych. Na gruncie polskim znalazło to wyraz w art. 129m u.p.p.p. Podmioty zobligowane do wpisu posiadają status instytucji obowiązanej, który zostanie omówiony w dalszej części artykułu. W tym miejscu można zadać pytanie o faktyczne korzyści płynące z funkcjonowania rejestru[31], w którym zgodnie ze stanem na 6 kwietnia 2023 r. było wpisanych 705 podmiotów deklarujących rodzaj świadczonych przez nie usług, tj. wymiany pomiędzy walutami wirtualnymi i środkami pieniężnymi, pomiędzy samymi walutami wirtualnymi, pośrednictwa w takiej wymianie oraz prowadzenia rachunków dla walut wirtualnych. Zdaniem autorów taki wpis, o charakterze deklaratoryjnym, obecnie bardziej służy firmom do uwierzytelnienia swej działalności, jako afirmowanej przez państwo, niż do faktycznej kontroli tych firm przez organy uprawnione na podstawie u.p.p.p.

---

[30] *Anti-money laundering: Provisional agreement reached on transparency of crypto asset tra*nsfers, Council of the EU, 29 VI 2022 r., https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [dostęp: 7 IV 2023].

[31] Zgodnie z ustawą rejestr jest prowadzony przez ministra finansów, a faktycznie zarządza nim Izba Administracji Skarbowej w Katowicach (rejestr znajduje się pod adresem: https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach).

Poszczególne kraje w różny sposób realizują obowiązki polityki AML/CFT, a priorytetem FATF jest to, aby zręby światowego systemu przeciwdziałania praniu pieniędzy były jednolite. W dokumentach FATF zaleca się stosowanie podejścia funkcjonalnego. Zgodnie z nim poszczególne kraje modelują szczegółowe rozwiązania prawne pod kątem ich wewnętrznych, specyficznych uwarunkowań, ale wszędzie implementacja zasadniczych wytycznych powinna być na niezmiennie wysokim poziomie. W UE to zadanie realizuje Komitet Ekspertów ds. Oceny Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu (Moneyval), który jest stałym organem monitorującym Rady Europy. Komitetowi powierzono ocenę zgodności norm krajowych z międzynarodowymi standardami AML/CFT, skuteczne wdrażanie tych unormowań, a także formułowanie zaleceń dla władz państwowych w sprawie poprawy przepisów obowiązujących na tym polu. Zalecenia FATF i Moneyval wymagają zatem tworzenia przez kraje sprawnych procedur AML, w tym nałożenia na uczestników rynku kryptoaktywów określonych zobowiązań, chociaż każdy rząd może indywidualnie konkretyzować przyjęte rozwiązania[32]. Determinantami w implementacji dyrektyw unijnych są takie czynniki, jak ustrój polityczny kraju, jego rozwój gospodarczy, otwartość danego społeczeństwa na innowacje i jego zamożność.

Finansowanie terroryzmu za pomocą kryptowalut

Kryptowaluty są powiązane z działalnością organizacji ekstremistycznych – co najmniej od 2015 r. odnotowywano terrorystów starających się wykorzystać bitcoiny do tworzenia zbiórek crowdfundingowych finansujących ich operacje[33]. W większości były one organizowane przez grupy operujące

[32] P. Opitek, *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 41–70, Lex, https://sip.lex.pl/komentarze-i-publikacje/artykuly/przeciwdzialanie-praniu-pieniedzy-z-wykorzystaniem-walut-151383722 [dostęp: 7 IV 2023].

[33] *Statement of Stephanie Dobitsch, Deputy Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security*, w: *Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee On Homeland Security House of Representatives*, 2021 r., https://www.congress.gov/117/chrg/CHRG-117hhrg45867/CHRG-117hhrg45867.pdf, s. 8 [dostęp: 10 V 2023]. Polskie służby ochrony prawa omawiały temat terroryzmu już w 2018 r., m.in. po prelekcji Pawła Opitka pt. *Wykorzystanie kryptowalut w przestępczości zorganizowanej i terroryzmie* przedstawionej podczas szkolenia prokuratorów Departamentu do Spraw Przestępczości

na terenie Bliskiego Wschodu, które cechują silne motywacje ideologiczne, ale do nielegalnych działań dotyczących kryptowalut i terroryzmu doszło także w Stanach Zjednoczonych, Europie Zachodniej, a ostatnio także w Ukrainie i Polsce. W raportach służb amerykańskich potwierdzono, że nowe technologie, takie jak kryptowaluty, umożliwiają terrorystom dalszą ekspansję i wspierają ich wysiłki w gromadzeniu środków finansowych na nielegalną działalność[34].

Do organizowania działań o charakterze terrorystycznym jest potrzebne wsparcie finansowe, a jego beneficjenci mogą otrzymywać pomoc w postaci kryptoaktywów. Finansowanie terroryzmu za pomocą walut wirtualnych wiąże się m.in. z fundamentalizmem islamskim i omijaniem sankcji ekonomicznych przez państwa nierespektujące w pełni reguł rynku finansowego narzucanych przez zachodnie, liberalne demokracje. W kręgach fundamentalistów islamskich toczyła się dyskusja, czy kryptowaluty są dozwolone przez szariat i czy muzułmanie powinni je wykorzystywać. Ostatecznie Al-Ka'ida opublikowała w Internecie latem 2014 r. manifest pt. *Bitcoin wa Sadaqat al-Jihad*[35]. Promowała w nim użycie bitcoina jako dogodnego środka wspierającego walkę z niewiernymi z pominięciem zachodniego systemu bankowego, który ograniczał darowizny na rzecz dżihadu. W manifeście zalecano realizowanie transferów kryptowalutowych z pobudek ideowych i religijnych, jak również opisano techniczne walory walut wirtualnych: odporność na fałszerstwa, anonimowość nadawców i odbiorców, globalny zasięg, trudności w wykryciu płatności przez organy ścigania. Podkreślono wyższość systemu Bitcoina nad takimi metodami, jak PayPal czy eBay, które są zarządzane odgórnie i mają charakter scentralizowany. Twórcom manifestu chodziło o stworzenie całkowicie anonimowego systemu do wysyłania darowizn w bitcoinach ze Stanów Zjednoczonych, Wielkiej Brytanii, Republiki Południowej Afryki, Ghany, Malezji, Sri Lanki lub innego miejsca na świecie na adres portfela DarkWallet zarządzanego przez mudżahedinów. Zapowiedziano opublikowanie takiego narzędzia (pojawiło się ono w 2019 r.). W konkluzji autorzy manifestu stwierdzili,

Zorganizowanej i Korupcji Prokuratury Krajowej oraz funkcjonariuszy Centralnego Biura Śledczego Policji i Agencji Bezpieczeństwa Wewnętrznego i przedstawicieli innych organów w zakresie zwalczania zagrożeń o charakterze terrorystycznym. Szkolenie odbyło się w Waplewie w dniach 5–7 listopada 2018 r.

[34] *Statement of Chairwoman Elissa Slotkin*, w: *Terrorism and Digital Financing*…, s. 3.

[35] *Bitcoin wa Sadaqat al-Jihad,* https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf [dostęp: 20 I 2019].

że chociaż wykorzystanie bitcoinów napotyka różne przeszkody, a większość kafirów wykorzystuje je do nabycia narkotyków, to jednak kryptoaktywo może zostać wykorzystane do realizacji wielu przydatnych celów: od zakupu broni po darowiznę dla mudżahedinów. Takie stanowisko było jedną z przyczyn powstania wielu stron w mediach społecznościowych organizujących zbiórki w kryptowalucie na rzecz terrorystów islamskich z różnych krajów i organizacji. Zbiórki są prowadzone nie tylko przez podmioty bezpośrednio powiązane z przestępcami, lecz także przez ich sympatyków mieszkających w Stanach Zjednoczonych czy Europie.

Al-Ka'ida od początku istnienia korzystała z forów i czatów w otwartym Internecie, jednak po zakrojonej na szeroką skalę akcji służb w 2000 r. i aresztowaniach kilku zwolenników dżihadu wiele platform przeniosło się do Darknetu. Obecnie zaawansowane fora dżihadystów chronią się przed inwigilacją służb szyfrowaniem kryptograficznym, stosują narzędzia typu Sigaint lub TorBox, a dostęp do platformy jest weryfikowany przez administratora. W Internecie powstają fora powiązane z radykalnymi ruchami, np. Shumukh al-Islam oscylujące pomiędzy zwolennikami ISIS i Al-Ka'idy[36]. W 2019 r. militarne skrzydło Hamasu – Brygady Izz ad-Din al-Kassam – zamieściło w mediach społecznościowych i na swoich stronach internetowych (alqassam.net, alqassam.ps, qassam.ps) wezwanie do składki w bitcoinach na „kampanię terroru". Jednocześnie przestępcy uczyli się zasad cyberbezpieczeństwa. Brygady te początkowo zażądały wysyłania kryptowaluty na jeden adres hostowany na amerykańskiej giełdzie, potem jednak opracowały technologię generowania dla każdej wpłaty indywidualnego adresu, aby utrudnić śledzenie pochodzenia i transferów środków. Wprowadzanie przez grupy terrorystyczne nowych rozwiązań wskazuje, że mogą one dostosowywać się do strategii minimalizujących ryzyko i wykorzystywać różne luki w zabezpieczeniach technologicznych[37]. Działalność cyberterrorystów nie ogranicza się tylko do crowdfundingu. Na początku 2021 r. media Al-Ka'idy zaoferowały nagrodę w wysokości 1 bitcoina, wartego wówczas 60 000 dolarów, osobie, która zamorduje policjanta w kraju zachodnim. Dwa lata wcześniej Brenton Tarrant, sprawca ataków na meczety w Christchurch w Nowej

[36] B. Berton, *The dark side of the web: ISIL's one-stop shop?*, European Union Institute for Security Studies, czerwiec 2015 r., https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [dostęp: 23 VIII 2019].

[37] *Risk Assessment. 2022 National Terrorist Financing*, Department of the Treasury, luty 2022 r., https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf, s. 22 [dostęp: 10 V 2023].

Zelandii, twierdził, że zarabiał na handlu kryptowalutami. W tym samym czasie działający z pobudek rasowych ekstremista, który usiłował dokonać zamachu w synagodze na terenie Niemiec, zeznał, że otrzymywał wsparcie finansowe w bitcoinach[38]. Wiele wskazuje na to, że sprawcy zamachów terrorystycznych przeprowadzonych 13 listopada 2015 r. w Paryżu byli wspierani podczas ich organizowania przekazami kryptowalutowymi[39].

Aktywność internetowych terrorystów została zauważona i rozpracowana przez amerykańskie służby ochrony prawa, które wypracowały najbardziej efektywne i zaawansowane narzędzia oraz metody zwalczania ekstremizmu w Internecie. W Stanach Zjednoczonych jednym z głównych organów publicznych zajmujących się walką z terroryzmem jest Departament Bezpieczeństwa Wewnętrznego (ang. Department of Homeland Security, DHS). Jego przedstawiciel podczas wysłuchania w Kongresie w 2021 r. stwierdził, że DHS wraz z Urzędem Skarbowym (ang. Internal Revenue Service, IRS) i Federalnym Biurem Śledczym (ang. Federal Bureau of Investigation, FBI) przeprowadził globalną operację cybernetyczną i zlikwidował infrastrukturę wirtualną Brygad Izz ad-Din al-Kassam. Począwszy od października 2019 r. działający pod przykryciem agenci Homeland Security Investigations (HSI), służby zajmującej się walką z terroryzmem, dokonywali na rzecz terrorystów darowizn w bitcoinach, aby rozpracować powiązania podmiotów prowadzących internetowe zbiórki na rzecz Hamasu. Te działania umożliwiły śledczym ustalenie zwolenników tej organizacji mieszkających w Stanach Zjednoczonych oraz przeprowadzenie dalszego śledzenia transferowanych środków. Zidentyfikowano 64 unikalne kanały komunikacji (m.in. adresy e-mail), co pozwoliło zabezpieczyć portfele bitcoinowe darczyńców. Operacja ujawniła modus operandi terrorystów w Internecie, w tym sposoby prowadzenia rekrutacji zwolenników w systemie online, metody finansowania, a także użytkowane przez nich domeny oraz infrastrukturę IT, funkcjonującą m.in. w Stanach Zjednoczonych, Kanadzie, Rosji, Niemczech i Arabii Saudyjskiej. W lipcu 2020 r. agenci specjalni HSI i IRS zrealizowali 24 federalne nakazy przeszukania, konfiskaty kryptowaluty i zabezpieczenia danych na licznych giełdach internetowych i u dostawców usług sieciowych – poczty elektronicznej, VPN-ów, płatności online. Zarekwirowano serwery, zamknięto wiele

[38] *Statement of Stephanie Dobitsch…*, s. 8.

[39] Zob. m.in. Y.B. Perez, *Bitcoin, Paris and Terrorism: What the Media Got Wrong*, CoinDesk, 6 III 2023 r., https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong [dostęp: 10 V 2023].

domen i skrzynek e-mail powiązanych z działalnością terrorystyczną. Do operacji w cyberprzestrzeni dołączyły zaprzyjaźnione służby na całym świecie, co pozwoliło przejąć terabajty danych kontrolowanych przez terrorystów, setki portfeli bitcoinowych, kryptoaktywa warte kilka milionów dolarów oraz zlikwidować strony przeznaczone do przekazywania datków w bitcoinach. Inne śledztwo z 2020 r., prowadzone przez HSI, IRS i FBI, miało związek z 24 kontami kryptowalutowymi zidentyfikowanymi jako zagraniczne aktywa lub źródła wpływów dla Al-Ka'idy. Cyberoperacja dotyczyła wykorzystania kryptowaluty do wspierania i finansowania terroryzmu, a w jej wyniku zostało przejętych 60 portfeli wirtualnych[40].

Działania ukierunkowane na zwalczanie finansowania terroryzmu z wykorzystaniem walut wirtualnych rząd Stanów Zjednoczonych traktuje jako ważny front walki z międzynarodowym terroryzmem. Potwierdza to dokument pt. *Krajowa strategia walki z terroryzmem i innym nielegalnym finansowaniem* z 2020 r.[41] przygotowany przez Departament Skarbu USA (ang. United States Department of the Treasury). Podniesiono w nim, że po atakach z 11 września 2001 r. tamtejsze władze skupiły się na słabych punktach systemu finansowego. Chodzi o nadużycia dokonywane przez organizacje charytatywne i nielicencjonowane przekazy pieniężne, które pozwoliły Al-Ka'idzie na międzynarodowe transfery pieniędzy w celu finansowania ataków terrorystycznych. Po zamachu na World Trade Center niektóre grupy ekstremistyczne porzuciły działania na skalę globalną

[40] *Statement of John Eisert, Assistant Director, Investigative Programs, Homeland Security Investigations, Immigration and Customs Enforcement, Department of Homeland Security*, w: *Terrorism and Digital Financing*..., s. 14–16. W 2021 r. Departament Sprawiedliwości USA ogłosił likwidację infrastruktury trzech kampanii przeprowadzonych w cyberprzestrzeni i służących finansowaniu terroryzmu, z udziałem Brygad Izz ad-Din al-Kassam będących wojskowym skrzydłem Hamasu, Al-Ka'idy oraz Islamskiego Państwa Iraku i Lewantu (ISIS). W tych kampaniach zostały wykorzystane wyrafinowane narzędzia cybernetyczne, m.in. pozyskano z całego świata darowizny w postaci kryptowalut. Akcja pokazała – jak głosił komunikat rządu USA – jak różne grupy terrorystyczne w podobny sposób dostosowały do ery cybernetycznej swoją działalność związaną z finansowaniem terroryzmu. Amerykańskie władze przejęły miliony dolarów powiązane z nielegalnym procederem, ponad 300 kont kryptowalutowych, cztery strony internetowe i cztery strony na Facebooku. Zob. *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*, The United States Department of Justice, 13 VIII 2020 r., https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [dostęp: 9 V 2023].

[41] *National Strategy for Combating Terrorist and Other Illicit Financing 2020*, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf [dostęp: 7 VII 2023].

(złożone i rozległe ataki), a skoncentrowały się na działalności pojedynczych terrorystów. Zradykalizowane osoby mogą przeprowadzać stosunkowo tanie i nieskomplikowane, ale skutkujące ofiarami ataki przy użyciu noży, broni palnej i samochodów. Tego rodzaju działaniom sprzyja komunikacja online i transfery kryptowalutowe dokonywane w ukryciu bezpośrednio do portfeli indywidualnych osób, co ogranicza ślad finansowy[42].

Jednak zagadnienie „kryptowaluty a ekstremizm" dotyczy nie tylko terrorystów, lecz także innych organizacji wywrotowych, zagrażających stabilności i bezpieczeństwu państw demokratycznych. Wirtualne zbiórki crowdfundingowe są wykorzystywane również przez organizacje neonazistowskie. Skrajnie prawicowi ekstremiści działający w Internecie używają kryptowalut m.in. dlatego, że są one kojarzone z ideologią głęboko zakorzenionej nieufności wobec instytucji finansowych, jako tych opanowanych i zarządzanych przez „żydowską finansjerę". Przemawiają do nich również libertariańskie początki filozofii związanej z powstaniem bitcoina wiążące się z niechęcią do światowego establishmentu. Nie mniej ważne są czysto praktyczne aspekty funkcjonowania kryptowalut. Amerykańscy neonaziści są rugowani z popularnych platform crowdfundingu typu Patreon, dlatego też tworzą alternatywne serwisy przeznaczone do dokonywania dotacji w formie zdecentralizowanych tokenów. W taki sposób powstał Hatreon. Firmy hostujące odmawiały jego utrzymania, więc zmieniał on domeny na coraz lepiej maskujące administratora platformy[43].

Zbiórkę kryptowalut prowadzi na przykład strona internetowa o nazwie *The Daily Stormer* redagowana przez amerykańskich neonazistów. Znajduje się na niej dokładna instrukcja, jak realizować przelewy bitmonet na podany tam adres, a zalecaną formą wpłat są kryptobankomaty. Andrew Anglin, główny redaktor tej strony, wydający także pismo o takim samym tytule, jest znanym aktywistą realizującym skuteczne akcje crowdfundingowe na cele swojej organizacji. Anglin wielokrotnie zachwalał, m.in. na łamach „The Washington Post", wirtualne waluty jako doskonałe narzędzie do gromadzenia środków na działalność zwalczaną przez władze państwowe oraz potwierdził, że otrzymał znaczne datki od osób wspierających jego projekty i ideologię.

---

[42] Tamże, s. 11–12.

[43] P. Opitek, *Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finasowania terroryzmu*, Warszawa 2019, s. 43–44 (praca dyplomowa napisana na studiach podyplomowych w Szkole Głównej Handlowej, niepublikowana, w zasobach autora).

Działania rekrutacyjne prowadzone przez dżihadystów w Internecie są często ściśle powiązane z apelami o pomoc finansową dla terrorystów opartą na crowdfundingu. Łatwość przekazywania funduszy i możliwość dotacji w postaci stosunkowo niewielkich kwot może pomóc materialnie organizacji ekstremistycznej, a aktywność darczyńcy pozostanie niezauważona przez system AML. Przykładem zrealizowanego crowdfundingu kryptowalutowego przeprowadzonego na rzecz bojowników tzw. Państwa Islamskiego była sprawa Alego Shukri Amina. Mężczyzna urodził się w Afryce i w wieku kilku lat wyemigrował z matką do Stanów Zjednoczonych. Zamieszkał w Wirginii i tam uczęszczał na studia. Interesowały go przedmioty ścisłe, tematy dotyczące cyberbezpieczeństwa, szyfrowania i kryptowalut. Jednocześnie Amin radykalizował się i propagował swoje idee w mediach społecznościowych. Założył m.in. konto na Twitterze o nazwie @AmreekiWitness, na którym zamieścił 7000 tweetów pochwalających radykalny islam i propagujących wsparcie finansowe dla ISIS za pomocą anonimowych transferów bitcoinowych. Stworzył ponadto blog Al-Khilafah Aridat, na którym zachęcał do walki z niewiernymi, jak również opracował serię artykułów adresowanych do zwolenników tzw. Państwa Islamskiego. Opisał w nich ze szczegółami, w jaki sposób komunikować się anonimowo w sieci i korzystać z szyfrowania podczas nielegalnej aktywności na rzecz terrorystów. Amin pomógł także znajomemu mężczyźnie dotrzeć przez Turcję do Syrii i przyłączyć się do bojowników islamskich. W 2015 r. prokurator skierował do sądu akt oskarżenia przeciwko niemu[44], w którym zarzucił mu angażowanie się wraz z innymi ustalonymi i nieustalonymi osobami w działalność terrorystyczną polegającą na udzieleniu wsparcia materialnego i fachowych porad zagranicznym terrorystom z ISIS. Mężczyzna został skazany przez sąd na karę 11 lat pozbawienia wolności.

Obowiązki instytucji obowiązanej w systemie przeciwdziałania praniu pieniędzy

Filarem walki z przestępstwem prania pieniędzy jest polityka AML, którą muszą prowadzić instytucje obowiązane. Są to podmioty uczestniczące

[44] *United States of America v. Ali Shukri Amin*, CRIMINAL NO. 1:15-CR-164, https://www.investigativeproject.org/documents/case_docs/2826.pdf [dostęp: 10 V 2023].

w szeroko rozumianym obrocie walutami wirtualnymi i z tego tytułu rządy poszczególnych państw nałożyły na nie określone obowiązki mające przeciwdziałać procederowi prania pieniędzy. Wiele działań AML dotyczących kryptoaktywów jest podobnych do tych, które od dawna są związane z płatnościami pieniądzem lub pieniądzem elektronicznym. Biorąc jednak pod uwagę specyfikę zarządzania ryzykiem transakcji angażujących tokeny cyfrowe, postuluje się konieczność przestrzegania w stosunku do rynku krypto wysokich wymagań dotyczących prowadzonej tam działalności, np. uzyskania zezwolenia na funkcjonowanie firmy, spełnienia wymogów ostrożnościowych w zakresie posiadania kapitału zakładowego gwarantującego płynność, prowadzenia transparentnej rachunkowości i dokonywania okresowych audytów, posiadania aktywów rezerwowych stanowiących równowartość wyemitowanych tokenów. Ten fundusz gwarancyjny, chroniący inwestorów, stanowi zabezpieczenie finansowe, gdyby doszło np. do zhakowania protokołu blockchaina i „kradzieży" bazującej na nim wartości. W związku z takimi cyberzagrożeniami instytucje obowiązane muszą przestrzegać wysokich wymagań chroniących posiadane aktywa, w tym klucze kryptograficzne, oraz stosować, wpisane w ład korporacyjny, profesjonalne systemy kontroli, zarządzania ryzykiem i raportowania. Dochodzą do tego wymagania w zakresie wewnętrznych procesów prowadzenia dokumentacji firmy, przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, bezpiecznego outsourcingu, odporności operacyjnej kluczowych usług (zapewnienie ciągłości funkcjonowania firmy i wysokiej jakości usług w przypadku awarii systemów elektronicznych lub takich zdarzeń fizycznych, jak pożar czy przerwanie dostaw energii elektrycznej). Trzeba również zmierzyć się z takimi wyzwaniami, jak przyjęcie stosownych regulacji dotyczących niewypłacalności i upadłości firmy, która ulokowała swój majątek w kryptoaktywach lub świadczyła usługi i sprzedawała produkty na rynku kryptograficznym[45].

Walka z praniem pieniędzy oraz przeciwdziałanie terroryzmowi, z uwzględnieniem walut wirtualnych, bazuje na wspólnych rozwiązaniach wdrażanych przez UE do porządków prawnych państw Unii. Szczególną rolę odegrała piąta dyrektywa w sprawie przeciwdziałania praniu pieniędzy

[45] *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf, s. 20–21 [dostęp: 9 IV 2023].

(UE) 2018/843[46], która weszła w życie w czerwcu 2018 r. W Polsce przepisy wprowadzające rozwiązania zawarte w tym akcie prawnym obowiązują od maja 2021 r.[47] Dyrektywy AML wydawane wspólnie przez Parlament Europejski i Radę UE kształtują prawa i obowiązki profesjonalnych uczestników rynku, organów administracji publicznej (m.in. jednostek analityki finansowej), a pośrednio oddziałują także na politykę kryminalną państwa. W tym ostatnim przypadku chodzi o możliwości egzekwowania obowiązków wobec instytucji obowiązanych, karania osób odpowiedzialnych za ich niewykonanie, wykorzystania źródeł dowodowych czy zabezpieczania majątku pochodzącego z przestępstwa.

Skorzystanie przez organy ścigania z możliwości, jakie stwarzają w Polsce przepisy u.p.p.p., wymaga znajomości mechanizmów, którymi system AML rządzi się w stosunku do instytucji obowiązanych, w tym podmiotów prowadzących działalność gospodarczą polegającą na świadczeniu usług w zakresie walut wirtualnych (art. 2 ust. 1 pkt 12 u.p.p.p.). Takie podmioty mają obowiązek sporządzenia i stosowania (a także aktualizowania i weryfikowania) wewnętrznej procedury w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, o której mowa w art. 50 u.p.p.p. Wskazany przepis enumeratywnie wymienia, co zawiera taka procedura, z uwzględnieniem charakteru, rodzaju i rozmiaru działalności prowadzonej przez przedsiębiorcę, a całe podejście do bezpieczeństwa finansowego opiera się na szacowaniu ryzyka. Tym ryzykiem jest możliwość zaktualizowana się zagrożenia (łącznie z możliwością popełnienia przestępstwa) w stosunku do konkretnego klienta instytucji obowiązanej w ramach świadczonych przez nią usług. Takie ryzyko może być określone jako minimalne i wtedy nie wymaga się stosowania szczególnych środków ostrożności. W momencie jednak, gdy ryzyko zostanie oszacowane jako wysokie, wdraża się wzmożone środki bezpieczeństwa finansowego (wnikliwe badanie źródła pochodzenia środków, ustalanie beneficjenta rzeczywistego), łącznie z możliwością zerwania przez instytucję obowiązaną relacji gospodarczych z klientem. Już teraz ocena zakresu i częstotliwości

[46] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE,* https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018L0843&from=en.

[47] *Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw.*

stosowania przedmiotowych środków ciąży na firmie kryptowalutowej, a planuje się dalsze zaostrzenie przepisów. W dniu 7 grudnia 2022 r. Rada UE uzgodniła stanowisko, zgodnie z którym w całej Unii będzie obowiązywać maksymalny limit płatności gotówkowych w wysokości 10 000 euro, a dodatkowo anonimowość transferów zostanie ograniczona w przypadku handlu kryptoaktywami, ponieważ wszyscy dostawcy takich usług będą zobowiązani do przeprowadzania badania *due diligence*, tj. szczegółowej oceny aktualnej sytuacji kontrahenta oraz określenia istniejącego i potencjalnego ryzyka związanego z planowaną operacją finansową w przypadku transakcji o wartości co najmniej 1000 euro[48]. Już teraz instytucja obowiązana powinna bliżej zainteresować się swoim klientem, gdy w jego aktywności na platformie pojawiają się typowe symptomy świadczące o możliwości prania pieniędzy przy użyciu kryptowalut. Chodzi m.in. o posługiwanie się wieloma rachunkami zarejestrowanymi na różne osoby, wielokrotne przewalutowanie środków zgromadzonych na rachunkach lub konwersję pomiędzy pieniądzem a walutami wirtualnymi bez sprecyzowanego celu biznesowego, korzystanie przez klienta z bankomatów, wpłatomatów, kryptobankomatów lub innych urządzeń umożliwiających anonimowe wpłaty lub wypłaty gotówki i walut wirtualnych bez racjonalnego uzasadnienia w profilu transakcyjnym danej osoby czy też o wykorzystywanie do transakcji (wejścia lub wyjścia środków) takich niestandardowych metod płatności, jak Mistertango, N26, Revolut, Western Union, Wirex, PayPal, MoneyGram[49]. Identyfikacja i ocena ryzyka AML/CFT powinna uwzględniać wiele czynników, m.in. dotyczących statusu klientów (kraj pochodzenia, wielkość firmy i profil jej działalności), państw lub obszarów geograficznych ich pochodzenia, rodzaju produktów i usług oferowanych przez kontrahentów oraz kanałów dystrybucji dóbr, rodzaju wykonywanych transakcji. Katalog badanych okoliczności nie jest zamknięty i podlega dostosowaniu do zmieniających się wewnętrznych i zewnętrznych uwarunkowań w otoczeniu podmiotu zaangażowanego w działalność kryptowalutową.

Pierwszy wniosek, jaki ABW lub inna służba specjalna prowadząca czynności powinna skierować do instytucji obowiązanej, której działalność pozostaje w zainteresowaniu tej służby, to zwrócenie się o przedłożenie

---

[48] *Fight against money laundering and terrorist financing*, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/ [dostęp: 9 IV 2023].

[49] E. Przewłoka, *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej*, Bydgoszcz 2023 (metodyka wewnętrzna Policji, w zbiorach autora).

wewnętrznej procedury w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu w celu sprawdzenia, jak ukształtowano tę procedurę, czy dokument spełnia wymogi prawa i odpowiada rzeczywistej działalności instytucji, a następnie zweryfikowania, jak wyglądała realizacja procedury w praktyce. Jeśli dokument jest rzetelny, to na jego podstawie wiadomo, kto za co odpowiadał w polityce AML danego podmiotu, jak szacowano ryzyko, gdzie znajdują się i co zawierają metadane gromadzone w trakcie kontaktów na odległość z kontrahentami. Można ponadto zwrócić się z zapytaniami dotyczącymi konkretnego klienta:

1. Czy w relacjach handlowych ukrywał on prawdziwe dane osobowe?
2. Czy posługiwał się rachunkiem (np. płatniczym, bankowym, walut wirtualnych) założonym na inną osobę lub podawał się za kogoś innego w kontaktach z pracownikami instytucji?
3. Czy przedkładał dokumenty wzbudzające zastrzeżenia co do ich autentyczności lub rzetelności?
4. Czy logował się na konta osób trzecich?
5. Czy odmawiał przedłożenia określonych dokumentów lub podania źródła pochodzenia środków, którymi dysponował?
6. Czy w jeszcze inny sposób utrudniał działanie instytucji obowiązanej w zakresie realizacji obowiązków AML?
7. Czy korzystał z wpłat lub wypłat bankomatowych z zaangażowaniem środków na giełdzie?[50]

Badaniu podlegają także inne dokumenty, które zgodnie z art. 50 ust. 2 u.p.p.p. stanowią obligatoryjne składniki wewnętrznej procedury AML instytucji obowiązanej, tj. zasady dotyczące stosowania środków bezpieczeństwa finansowego, przechowywania dokumentów oraz informacji, wykonywania obowiązków obejmujących przekazywanie Generalnemu Inspektorowi Informacji Finansowej (GIIF) informacji o transakcjach oraz zawiadomieniach, upowszechniania wśród pracowników instytucji obowiązanej wiedzy z zakresu przepisów o przeciwdziałaniu praniu pieniędzy oraz zgłaszania przez pracowników rzeczywistych lub potencjalnych naruszeń tych przepisów, audytu wewnętrznego.

Obowiązki wpisane w politykę AML instytucji obowiązanej dotyczą także analizy samych transakcji dokonywanych przy użyciu walut wirtualnych. Prokurator może zażądać od giełdy przedstawienia w formie analitycznej informacji dotyczących historii zleceń klienta (wejścia i wyjścia środków),

[50] Tamże.

usług i produktów finansowych lub kryptowalutowych (zwłaszcza nietypowych), z jakich korzystał klient, przedłożenia indywidualnej (obowiązującej aktualnie oraz w przeszłości, jeśli ulegała zmianie) oceny ryzyka przypisanego danej osobie lub instytucji, sprawdzenia, czy przelewała ona lub próbowała przelać środki do rajów podatkowych lub krajów objętych sankcjami. W stanie prawnym na dzień 21 marca 2023 r. kryptoaktywa są objęte sankcjami nałożonymi na Rosję, a więc przepisami dotyczącymi zamrożenia majątku określonych osób, zakazu ich udostępniania przez te osoby oraz jakiegokolwiek wykorzystania w celach gospodarczych. Kryptoaktywa nie powinny być także używane do obchodzenia jakichkolwiek sankcji ustanowionych na podstawie rozporządzenia Rady UE nr 833/2014[51]. Podmiotom z Unii zakazuje się ponadto świadczenia usług związanych z prowadzeniem lub dostarczaniem portfeli kryptowalutowych, rachunków lub usług powierniczych związanych z wartościami krypto zarówno obywatelom Rosji, jak i osobom fizycznym zamieszkałym na obszarze Federacji Rosyjskiej, a ponadto osobom prawnym oraz innym podmiotom mającym tam siedzibę. To oznacza, że europejscy dostarczyciele usług powinni zamknąć konta kryptograficzne swoich rosyjskich klientów i zwrócić im cyfrowe aktywa (ewentualnie zamienić je na pieniądze lub inną kategorię aktywów, które nie podlegają sankcjom), a w przypadku osób objętych sankcjami – zamrozić ich majątek. Przepisy sankcyjne należy odczytywać w powiązaniu z limitem depozytów określonym w art. 5b wspomnianego rozporządzenia i w tym zakresie zamiana kryptoaktywów na depozyty fiducjarne byłaby możliwa jedynie do wysokości kwoty dozwolonej dla depozytów[52].

Otwarta pozostaje odpowiedź na pytanie, jak skuteczne w praktyce są sankcje nałożone na Rosję. Według raportu renomowanej firmy analitycznej Inca Digital, wykonanego na podstawie analizy danych zebranych ze 163 platform handlu kryptowalutami na całym świecie, w tym scentralizowanych i zdecentralizowanych giełd i stron P2P oraz dostawców usług pozagiełdowych (ang. *Over the Counter Broker*, OTC[53]), aż 79 z nich umożliwia

---

[51] *Rozporządzenie Rady (UE) NR 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie.*

[52] *Crypto-assets. Relevant provision: Article 5b(2) of Council regulation (EU) NO 833/2014*, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [dostęp: 10 IV 2023].

[53] Nazwa oznacza usługi świadczone przez brokerów OTC, którymi są przede wszystkim duże giełdy kryptowalutowe typu Kraken, Binance, Coinbase, Satstreet, ułatwiające bezpośredni handel kryptowalutą pomiędzy dwoma stronami transakcji typu: krypto–krypto

obywatelom Rosji zakup kryptowaluty (zwłaszcza stablecoina Tether w systemie P2P), a 11 z 62 międzynarodowych platform nie ma przed rozpoczęciem handlu żadnych wymagań w stosunku do Rosjan w zakresie spełnienia procedury KYC[54]. Najbardziej przyjazne dla nich oraz najczęściej wykorzystywane są giełdy Huobi i KuCoin z siedzibą na Seszelach. Nie podjęły one żadnych kroków, aby uniemożliwić rosyjskim bankom objętym sankcjami korzystanie ze swoich platform i nieprzerwanie pozwalają na realizację transakcji kartami debetowymi wydanymi przez te banki, w tym Sbierbank. Według Inca Digital także Binance oferuje Rosjanom różne metody konwersji posiadanej przez nich waluty na krypto, m.in. za pomocą systemu OTC i rynku P2P, z pominięciem procedury KYC do równowartości depozytu w wysokości 10 tys. dolarów, ale ten limit jest łatwy do obejścia. Transakcje mogą być ukrywane m.in. poprzez kwalifikowanie płatności na rzecz nierosyjskich przedsiębiorstw użyteczności publicznej. ByBit operujący z Singapuru umożliwia użytkownikom wymianę rosyjskich rubli na kryptowaluty za pomocą rynku P2P i depozytu fiducjarnego. Opisana sytuacja jest bezpośrednim naruszeniem amerykańskich i europejskich sankcji i potwierdza, że analizowany rynek stanowi lukę w systemie ograniczającym możliwości gospodarcze Rosji. Chociaż z powodu nałożonych sankcji wiele giełd oficjalnie ograniczyło swoją działalność w tym kraju oraz deklaruje blokowanie użytkownikom z Rosji dostępu do oferowanych usług, to w rzeczywistości kontynuują one w mniej lub bardziej zawoalowanej formie współpracę z rosyjskimi obywatelami, m.in. umożliwiając im korzystanie z maksymalnych limitów wpłat, handlu i wypłat[55].

(np. wymiana bitcoina na ethereum) lub krypto–pieniądz fiducjarny. Handlowcy dysponujący dużymi wartościami majątkowymi poszukują bowiem bezpiecznych i anonimowych kanałów nieograniczonej limitami wymiany wartości majątkowych, na z góry ustalonych warunkach, które nie są formalnie notowane na scentralizowanych giełdach. Negocjowanie transakcji za pośrednictwem brokerów OTC pomiędzy sprzedającymi i kupującymi może odbywać się przez telefon lub sieć internetową, a nawet przewidywać osobiste spotkanie stron.

[54] *How Russians Use Tether to Evade Global Sanctions*, Inca Digital, https://inca.digital/intelligence/how-russians-use-tether/ [dostęp: 10 IV 2023].

[55] S. Sutton, L. Seligman, *Two major crypto exchanges failed to block sanctioned Russians*, Politico, 24 II 2023 r., https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391 [dostęp: 10 IV 2023]; *Crypto exchanges Huobi, KuCoin enabled Russian sanction evasion. Binance also mentioned*, Ledger Insights, 28 II 2023 r., https://www.ledgerinsights.com/russia-sanctions-crypto-exchanges-huobi-kucoin-binance/ [dostęp: 10 IV 2023].

Immanentną cechą związaną z obrotem walutami wirtualnymi jest utrudniony dostęp do informacji o podmiotach zaangażowanych w operacje, gdyż zazwyczaj działają one za pośrednictwem Internetu. Dlatego w przepisach prawnych położono nacisk na to, aby kontrolować ślad cyfrowy takiej działalności. 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 może pozwolić na ustalenie wielu istotnych danych o osobie pozostającej w jego zainteresowaniu, np. geolokalizację urządzeń elektronicznych, z których korzystała, oraz częstotliwość i czas lub okres jej kontaktów z instytucją obowiązaną. Dodatkowa analiza adresów IP w świetle zgromadzonego materiału dowodowego może udowodnić, że:

- transakcje realizowano z IP uprzednio wykorzystanych do nielegalnych działań (np. oszustw, ataków phishingowych, dystrybucji złośliwego oprogramowania typu ransomware);
- transakcji dokonywano z krajów objętych sankcjami, rajów podatkowych lub z innego „egzotycznego" terytorium lub państw wspierających międzynarodowy terroryzm;
- osoba pozostająca w zainteresowaniu organów ścigania używała narzędzi anonimizujących ruch sieciowy (Tor, VPN-y, proxy);
- zachodzą rozbieżności między adresami IP powiązanymi z profilem klienta a tymi, z których inicjowano transakcje (można z tego wnioskować, że osoba objęta śledztwem była tzw. słupem, a jej dane osobowe wykorzystał rzeczywisty beneficjent transakcji)[56].

Transakcje krypto należy zakwalifikować do kategorii podwyższonego ryzyka i szczegółowo analizować. W celu zwiększenia ich przejrzystości 29 czerwca 2022 r. Rada i Parlament UE osiągnęły wstępne porozumienie dotyczące aktualizacji unijnego rozporządzenia w sprawie informacji towarzyszących przekazom pieniężnym. Nowe przepisy wprowadzą obowiązek zbierania i udostępniania określonych informacji o nadawcach i beneficjentach transferów przez dostawców usług w zakresie aktywów kryptograficznych. Ma to zapewnić transparentność transferów kryptowalut, aby

[56] J. Skała, *Uzyskiwanie przez prokuratora informacji i danych od instytucji obowiązanych na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, z. 3, s. 92–93. https://doi.org/10.53024/4.3.47.2022.

móc lepiej identyfikować podejrzane operacje i blokować zaangażowane w nie środki[57]. To podwyższone ryzyko związane z anonimowością transakji krypto obejmuje oprócz typowych VASP także innych uczestników rynku finansowego (w tym banki), którzy co prawda nie biorą udziału w obrocie walutami wirtualnymi, ale pośrednio są narażeni na proceder prania pieniędzy z wykorzystaniem kryptoaktywów, gdyż np. prowadzą rachunki bankowe, na których są gromadzone środki pieniężne pochodzące z wymiany cyfrowych tokenów na pieniądz fiducjarny.

Ważną kategorię obowiązków nałożonych na instytucje stanowi powiadamianie właściwych organów państwowych o zdarzeniach mogących stanowić przestępstwo lub próbę jego dokonania oraz powiadamianie o charakterze sprawozdawczym. W ostatnim przypadku chodzi o przekazywanie GIIF informacji o przyjętych wpłatach i wypłatach środków pieniężnych, transakcjach dewizowych i transferach przekraczających próg o określonej wartości pieniężnej, a więc o transakcjach ponadprogowych (art. 72 u.p.p.p.). Instytucje obowiązane zawiadamiają także GIIF o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu (art. 74 u.p.p.p.) oraz przypadkach powzięcia uzasadnionego podejrzenia, że zlecenie przelewu lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu (art. 86 u.p.p.p.). W takiej sytuacji administrator platformy dokonuje blokady środków objętych zawiadomieniem, a dalsze decyzje o losie aktywów podejmuje prokurator zawiadomiony przez GIIF. Ponadto art. 89 u.p.p.p. reguluje obowiązek zawiadomienia właściwego prokuratora o powzięciu uzasadnionego podejrzenia, że wartości majątkowe będące przedmiotem transakcji lub zgromadzone na rachunku pochodzą z przestępstwa innego niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub z przestępstwa skarbowego albo mają związek z przestępstwem innym niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub z przestępstwem skarbowym. Wskazane procedury „blokad" są szczegółowo opisane w wymienionych artykułach, ale warto zwrócić uwagę na brzmienie niektórych instytucji prawnych opisanych w ustawie.

[57] *Fight against money laundering and terrorist financing…*

Określenie statusu cyfrowego artefaktu w postępowaniu karnym

W sytuacji gdy jakieś kryptoaktywo znajdzie się w obszarze zainteresowania organu ścigania, należy ustalić jego status techniczny i prawny. Od tego zależą bowiem ważne kwestie, m.in. możliwość wypełnienia znamion przestępstwa poprzez samo posiadanie lub emisję tokenów (np. zabroniona tokenizacja papierów wartościowych), sposób przejęcia faktycznego władztwa nad mieniem cyfrowym (czy kryptoaktywa są umieszczone na blockchainie publicznym lub prywatnym, a może w ogóle nie mają nic wspólnego z technikami łańcucha bloków), możliwość poszukiwania śladów popełnionego przestępstwa (umiejscowienie serwera). Określenie wspomnianego statusu nie zawsze jest łatwe i chociaż największa liczba spraw dotyczy bitcoinów lub podobnych altcoinów (ethereum czy litecoina), to zdarzają się sytuacje, w których ustalenie wszystkich cech tokena stanowi spore wyzwanie. Działo się tak w przypadku salonów prowadzących nielegalne gry hazardowe, w których gracze nabywali za pieniądze punkty do gry w formie cyfrowego odwzorowania ich wartości w kodzie QR. Badania pokazują, że polscy użytkownicy kryptoaktywów mają w swoich portfelach zaawansowane tokeny, których emisja na krajowym rynku kapitałowym jest obwarowana licznymi wymogami prawnymi, poddana nadzorowi organów regulacyjnych, a często nawet zabroniona. Chodzi m.in. o takie cyfrowe aktywa charakterystyczne dla rynku DeFi, jak PAXGOLD, USDT, COMP[58]. Większość użytkowników zadeklarowała ponadto, że korzystała z tokenów udziałowych podobnych do akcji lub obligacji, pochodnych instrumentów finansowych w formie kryptoaktywów lub inwestowała w takie instrumenty, a prawie połowa posiadała tokeny przypominające opcje, kontrakty terminowe lub swapy[59].

Scentralizowany i zdecentralizowany rynek kryptoaktywów rozrasta się, a organy publiczne, nie tylko w Polsce, lecz także na świecie, mają duże problemy z poruszaniem się po nim i egzekwowaniem obowiązków prawnych nałożonych na uczestników tego rynku. Należy przypuszczać, że czyny zabronione w postaci malwersacji finansowych czy prania pieniędzy dokonywane w środowisku takim jak DeFi zbyt często pozostają poza jakąkolwiek kontrolą państw i rządów. Autorzy artykułu nie znają sprawy, w której polskie organy ścigania lub nadzoru nad rynkiem kapitałowym przeprowadziły zaawansowane czynności związane z nadużyciami na rynku zdecentralizowanych finansów. Efektywne działania na tym polu podejmuje natomiast

[58] P. Opitek, *Funkcjonowanie instrumentów finansowych…*, s. 235.

[59] Tamże.

amerykański organ nadzoru nad rynkiem finansowym – Komisja Nadzoru nad Rynkiem Papierów Wartościowych i Giełd (ang. The Securities and Exchange Commission, SEC). W sierpniu 2021 r. oskarżyła ona przed sądem osoby odpowiedzialne o prowadzenie niezarejestrowanej w SEC sprzedaży papierów wartościowych za kwotę ponad 30 mln dolarów przy użyciu inteligentnych kontraktów i technologii zdecentralizowanych finansów, a także o wprowadzanie inwestorów w błąd w zakresie faktycznej rentowności oferowanych produktów. Oskarżeni działali jako firma Blockchain Credit Partners i emitowali oraz oferowali do sprzedaży na platformie DeFi Money Market dwa rodzaje tokenów o nazwie mTokeny i znacznej stopie zwrotu oraz tokeny DMG dające prawo głosu w wirtualnej spółce (DAO)[60]. Agencja regulująca rynek kontraktów futures (ang. The Commodity Futures Trading Commission, CFTC) w marcu 2023 r. oskarżyła w postępowaniu cywilnym przed sądem federalnym holding Binance, największą na świecie platformę do handlu walutami wirtualnymi, oraz jego dyrektora Changpenga Zhao o to, że bez wymaganej przez prawo rejestracji w CFTC oferował do sprzedaży obywatelom Stanów Zjednoczonych instrumenty pochodne w formie tokenów cyfrowych[61].

Innym przykładem na różnorodność „cyfrowych wartości" występujących w świecie wirtualnym są gry komputerowe, szczególnie te prowadzone w trybie online. Artefakty w grach mogą przedstawiać postacie ludzkie, broń (miecze, pistolety), amunicję, części zbroi, przedmioty ukrywające inne rzeczy (skrzynie, sejfy) lub bardziej abstrakcyjne elementy, których funkcja stanowi jakąś wartość dla użytkowników danej platformy. Znane są sytuacje, gdy artefakty w grach były wykorzystywane do prania pieniędzy[62] czy stanowiły przedmiot zamachu[63] lub działań wspierających terroryzm. W przypadku

[60] *SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings*, U.S. Securities and Exchange Commission, https://www.sec.gov/news/press-release/2021-145 [dostęp: 24 III 2023].

[61] *CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange*, CFTC, 27 III 2023 r., https://www.cftc.gov/PressRoom/PressReleases/8680-23 [dostęp: 5 IV 2023].

[62] P. Opitek, *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji*, „Przegląd Policyjny" 2017, nr 2, s. 150. https://doi.org/10.5604/01.3001.0013.6082.

[63] Wyrokiem Sądu Rejonowego dla Krakowa-Krowodrzy II Wydział Karny z 3 VIII 2012 r., sygn. akt II Ka 776/11/K, oskarżony został skazany za to, że w dniu 6 II 2011 r. w K. w celu osiągnięcia korzyści majątkowej, bez upoważnienia wpłynął na przesyłanie informacji poprzez przełamanie elektronicznego zabezpieczenia w ten sposób, że zmienił hasło dostępowe do skrzynki poczty elektronicznej o nazwie '...@poczta.onet.pl' należącej do T. K.,

podejrzenia, że wchodzą one w zakres modus operandi sprawcy przestępstwa, należy dokładnie ustalić status prawny takich „wartości". Przykładem na to, jak duże znaczenie ma właściwa ocena charakteru artefaktu, a pomyłka może dyskredytować prokuratora, jest sprawa dotycząca tzw. skinów, która zawisła przed sądem. Oskarżony został uznany przez Sąd Rejonowy w Przasnyszu[64] winnym popełnienia przestępstwa z art. 107 Kodeksu karnego skarbowego[65] w zw. z art. 29a ust. 1 i w zw. z art. 2 ust. 1 *Ustawy z dnia 19 listopada 2009 r. o grach hazardowych* (w brzmieniu sprzed 1 kwietnia 2017 r.), polegającego na tym, że w latach 2016–2017 organizował na platformach internetowych gry hazardowe o charakterze losowym, w których przedmiotem wygranej były wspomniane skiny. Stanowią one rodzaj funkcji używanej w grze *Counter-Strike: Global Offensive* w postaci różnego rodzaju broni, którą gracz może wypożyczyć i w taki sposób zmienić wygląd artefaktów stosowanych w grze[66]. Osoby, które uczestniczyły w losowaniu urządzanym przez oskarżonego, przekazywały do wirtualnego bębna swoje skiny. Następnie były one mieszane i w zależności od regulaminu obowiązującego na danej platformie wybrany losowo uczestnik otrzymywał największą liczbę skinów, a oskarżony pobierał prowizję z tytułu organizacji gry.

W brzmieniu sprzed 1 kwietnia 2017 r. art. 2 ust. 1 ustawy o grach hazardowych stanowił, że (...) *grami losowymi są gry, w tym urządzane przez sieć Internet, o wygrane pieniężne lub rzeczowe, których wynik w szczególności zależy od przypadku*. Tak więc warunkiem wypełnienia przez sprawcę znamion przestępstwa było uznanie przez sąd, że skin stanowi pieniądz lub rzecz[67]. W apelacji złożonej od wyroku skazującego obrońca oskarżonego podniósł, że skin nie może być traktowany jak pieniądz, gdyż nie jest emitowany przez Narodowy Bank Polski, nie jest także przedmiotem materialnym, a jedynie fragmentem kodu programistycznego, nie spełnia zatem definicji

po czym przejął jego postać w grze Metin 2 o nazwie „Joker 78", czym doprowadził T. K. do niekorzystnego rozporządzenia mieniem w kwocie nie mniejszej niż 500 zł, tj. o czyn z art. 287 § 1 k.k.

64 Akta sprawy Sądu Rejonowego w Przasnyszu II Wydział Karny, sygn. akt II K 608/18.

65 *Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy*.

66 https://counterstrike.fandom.com/wiki/Skins [dostęp: 17 II 2022].

67 W zarzucie znajdującym się w akcie oskarżenia i wyroku sądu I instancji napisano, że „ryzyku poddawane są tzw. skiny – wirtualne klucze posiadające w świecie rzeczywistym realną wartość pieniężną i umożliwiające dostęp do wirtualnej broni o różnej sile rażenia i osprzętów wykorzystywanych w walkach gry zręcznościowej 3D o nazwie Counter-Strike Global Offensive (w skrócie CS: GO) oferowane w ramach platformy społecznościowej STEAM należącej do Valve Corporation z siedzibą w Bellevue, Waszyngton, USA".

rzeczy z art. 45 Kodeksu cywilnego[68]. Sąd Okręgowy w Ostrołęce II Wydział Karny[69] podzielił argumentację zawartą w apelacji i wyrokiem z 27 sierpnia 2020 r. uniewinnił oskarżonego od popełnienia zarzucanego mu czynu. W uzasadnieniu wyroku sąd wskazał, że przepisów art. 2 ust. 1 pkt 1 ustawy nie można interpretować rozszerzająco i przez analogię, a oczywiste jest, że skiny nie mają statusu rzeczy lub przedmiotu, są bowiem wirtualnymi wartościami[70].

W ustaleniu statusu prawnego tokena podstawowe znaczenie ma udzielenie odpowiedzi na pytanie, czy stanowi on walutę wirtualną, której definicja legalna znajduje się w art. 2 ust. 2 pkt 26 u.p.p.p. Przeprowadzenie takiej oceny i udzielenie jednoznacznej odpowiedzi, czy dane aktywo podlega reżimowi ustawy AML, może okazać się bardzo trudne, m.in. dlatego że wspomniana definicja jest bardzo pojemna, a użyte w niej zwroty są nieostre[71]. Zakwalifikowanie tokena do walut wirtualnych powoduje, że organy ścigania mogą egzekwować względem instytucji obowiązanej zajmującej się obrotem taką walutą wiele obowiązków związanych z udzieleniem informacji o podejrzanych osobach i transakcjach. Na żądanie organu ścigania instytucja obowiązana powinna dostarczyć pełnych danych uzyskanych podczas pierwszej i kolejnych weryfikacji klienta (KYC) oraz historie wykonanych przez niego transakcji, wiadomości o ewentualnym raportowaniu do GIIF alertów o podejrzanych operacjach czy bazę numerów IP, które zostały wykorzystane do popełnienia przestępstwa. Podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług w zakresie wymiany pomiędzy walutami wirtualnymi i środkami płatniczymi czy konwersji pomiędzy samymi tokenami mają ponadto obowiązek przedłożenia na żądanie organów ścigania dokumentacji określonej w ustawie AML, m.in. przyjętej procedury szacowania ryzyka i przypisania poziomu ryzyka

[68] *Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny*.

[69] Sygn. akt II Ka 40/20.

[70] W obowiązującym stanie prawnym takie zachowanie stanowiłoby przestępstwo na podstawie art. 2 ust. 5 zmienionego *Ustawą z dnia 15 grudnia 2016 r. o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw* (DzU z 2017 r. poz. 88), który uzyskał brzmienie: „Grami na automatach są także gry na urządzeniach mechanicznych, elektromechanicznych lub elektronicznych, w tym komputerowych, oraz gry odpowiadające zasadom gier na automatach urządzane przez sieć Internet organizowane w celach komercyjnych, w których grający nie ma możliwości uzyskania wygranej pieniężnej lub rzeczowej, ale gra ma charakter losowy".

[71] Szczegółowe omówienie poszczególnych składników definicji terminu „waluty wirtualne" zob. w: G. Ocieczek, P. Opitek, *Analiza definicji walut wirtualnych z ustawy*..., s. 122–139.

konkretnemu klientowi[72]. Omówienie wszystkich środków i źródeł dowodowych, które można wykorzystać w śledztwie dotyczącym kryptowalut, wykracza poza ramy niniejszego opracowania, ale pewne jest, że u.p.p.p. daje organom ścigania duże możliwości działania. Funkcjonariusze znają je słabo i zbyt rzadko z nich korzystają.

Praca operacyjna w ramach zwalczania przestępczości kryptowalutowej

Doświadczenie nabyte w pracy prokuratora pokazuje, że niejawne działania pozaprocesowe stanowią niezbędny element skutecznej walki z przestępczością kryptowalutową. Dzieje się tak z kilku powodów. Sprawcy popełniający takie czyny zabronione są bardzo ostrożni i funkcjonują zazwyczaj w środowisku osób co najmniej tak hermetycznym jak zorganizowane grupy trudniące się handlem narkotykami czy bojówki pseudokibiców. Wynika to z tego, że zaplecze logistyczne do obrotu kryptowalutami jest dostępne zdalnie, a więc osoby z niego korzystające działają w świecie wirtualnym, do którego akces może być nieodwracalnie utracony wraz z zamknięciem matrycy ich laptopa. To jeden z powodów, dla których w ostatnich latach przewartościowaniu uległa metodyka prowadzenia przeszukania miejsc zajmowanych przez podejrzanych i zabezpieczania należącego do nich sprzętu elektronicznego. Wcześniej niepodważalna zasada głosiła, że funkcjonariusz uczestniczący w przeszukaniu, w trakcie którego ujawniono pracującą jednostkę komputera, nie powinien sam dokonywać przeszukania pamięci urządzenia, gdyż zmieni zapis danych w laptopie, co negatywnie przełoży się na wartość dowodową uzyskanych z niego śladów. Dzisiaj przeszukanie mieszkania lub zatrzymanie osoby nierzadko jest poprzedzone czynnościami operacyjnymi ukierunkowanymi na to, aby w momencie ich realizacji ujawnić i przejąć otwarty komputer sprawcy. Daje to możliwość uzyskania dostępu do wielu cennych informacji i danych zapisanych w pamięci urządzenia lub zasobach chmurowych, z którymi się łączy. W taki sposób można przejąć, tytułem zabezpieczenia majątkowego, cyfrowe mienie, uzyskać hasła dostępu do aplikacji wykorzystywanych do popełniania przestępstw lub do konta na giełdzie

[72] Szczegółowe omówienie źródeł dowodowych, które organy ścigania mogą wykorzystać w działaniach procesowych i operacyjnych związanych z walutami wirtualnymi, jest dostępne w: J. Skała, *Uzyskiwanie przez prokuratora informacji i danych*...

kryptowalutowej, sprawdzić, z jakich stron oraz serwisów internetowych korzystał sprawca, poznać treść rozmów prowadzonych przez niego za pomocą komunikatorów. Jeśli komputer zostanie zamknięty, to jest prawdopodobne, że biegły z zakresu informatyki śledczej nie będzie w stanie przełamać hasła zabezpieczającego dostęp do urządzenia, a nawet jeśli je uruchomi, to i tak zostaną utracone dane zapisane w ulotnej pamięci operacyjnej RAM czy dostęp do artefaktów przechowywanych przez przestępcę na innych serwerach.

Działania podejmowane w celu przejęcia otwartego komputera mogą mieć różny charakter, od podstępu (np. wejście do mieszkania „na listonosza"), przez pułapkę kryminalistyczną (sprowokowanie przestępcy do otworzenia laptopa w miejscu publicznym, co umożliwi jego przejęcie), aż po wykorzystanie zaawansowanych czynności operacyjno-rozpoznawczych. Może je poprzedzać zakamuflowana obserwacja osób i miejsc, wywiad posesyjny czy współpraca z dostawcą usług sieciowych, którego abonentem jest osoba podejrzewana. W grę wchodzi także kontrola operacyjna, zakup kontrolowany i przesyłka niejawnie nadzorowana. Zdarzało się, że organy ścigania nabywały bitcoiny, zakładały własne konta w darkmarkecie i kupowały narkotyki oferowane na platformie po to, aby ustalić kanały przesyłania zabronionych substancji, sposób ich dostawy oraz uzyskać quasi-opinię kryminalistyczną z zakresu badań fizykochemicznych, jak również ustalić, z jakimi środkami mają do czynienia w świetle ustawy o narkomanii[73].

Skuteczność niejawnych operacji w cyberprzestrzeni ukierunkowanych na zwalczanie przestępczości powiązanej z kryptowalutami potwierdzają doświadczenia służb amerykańskich. Chodzi m.in. o wykorzystanie funkcjonariusza operującego w Internecie pod przykryciem czy ustalanie położenia i zamykanie serwerów przechowujących nielegalne treści. Fizyczne przejęcie serwera to duży sukces, gdyż znajdują się na nim ślady będące dla organów ścigania źródłem wielu cennych informacji o setkach osób prowadzących nielegalną działalność z wykorzystaniem infrastruktury IT. Takie przejęcie to jednak niemałe wyzwanie i zazwyczaj jest ono możliwe tylko w ramach współpracy międzynarodowej. W dniu 28 lutego 2023 r. policje niemiecka i ukraińska, przy wsparciu Europolu, policji holenderskiej i FBI, aresztowały członków grupy przestępczej odpowiedzialnej za cyberataki typu ransomware bazujące na oprogramowaniu Doppel-Paymer oraz Dridex i ukierunkowane na infrastrukturę krytyczną firm

[73] *Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii.*

prywatnych. Oprogramowanie ransomware było dystrybuowane różnymi kanałami, w tym metodą phishingu i za pomocą załączonych do spamu dokumentów zawierających złośliwy kod JavaScript lub VBScript. Jednego z najpoważniejszych ataków dokonano na Szpital Uniwersytecki w Düsseldorfie, a w Stanach Zjednoczonych ofiary zapłaciły co najmniej 40 mln euro w kryptowalucie za odszyfrowanie danych[74]. Cechy ransomware są przyrównywane do ataków terrorystycznych, gdyż stanowią poważne zagrożenie bezpieczeństwa narodowego. Podobnie jak terroryzm ransomware koncentruje się na celach miękkich, takich jak cywilna infrastruktura krytyczna, ale w przeciwieństwie do terroryzmu jest motywowany przede wszystkim względami finansowymi[75]. Niekiedy jednak trudno jest postawić wyraźną granicę pomiędzy tymi dwoma cyberzagrożeniami. Na przykład rząd Korei Północnej jest odpowiedzialny za wiele poważnych ataków ransomware na infrastrukturę krytyczną na całym świecie. W 2021 r. Departament Sprawiedliwości Stanów Zjednoczonych ogłosił akt oskarżenia dotyczący trzech urzędników rządu Korei Północnej podejrzanych o przeprowadzenie kilku najniebezpieczniejszych cyberataków, m.in. WannaCry 2.0 (okup za odszyfrowanie danych płacono w kryptowalucie), włamanie do bazy danych Sony Pictures oraz do Banku Bangladeszu. W akcie oskarżenia zarzucono, że hakerzy są członkami koreańskiego wywiadu wojskowego, powiązanego z grupą hakerską o nazwie Lazarus, od lat zaangażowanego w operacje w cyberprzestrzeni[76]. Ślad koreański przypisywano także zaawansowanemu

---

[74] *Germany and Ukraine hit two high-value ransomware targets,* Europol, https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets [dostęp: 6 IV 2023]. Elissa Slotkin, przewodnicząca ds. Wywiadu i Kontrwywiadu Kongresu USA, w trakcie zeznań przed Kongresem w 2021 r. powiedziała o dokonanych wówczas w Stanach Zjednoczonych atakach terrorystycznych ransomware, „które uderzyły w serce życia codziennego w Ameryce, od gazociągów i przetwórstwa mięsnego i roślin, po funkcjonowanie szkół i szpitali", a na jej spotkaniu z wyborcami „pierwsze pytania rolników dotyczyły cyberataków, kryptowaluty i tego, co rząd zrobił, żeby ich chronić". Zob. *Statement of Chairwoman Elissa Slotkin*..., s. 2.

[75] *Ransomware Attacks on Critical Infrastructure Sectors,* U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf, s. i [dostęp: 11 V 2023].

[76] M. Dugas, *The Latest North Korea Cyber Indictment Should Serve as a Model,* Just Security, 24 II 2021 r., https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/ [dostęp: 11 V 2023]. W akcie oskarżenia ustalono, że Korea Północna w wyniku cyberterroryzmu, tj. włamań do banków, kradzieży kryptowalut, zarobiła łącznie ponad 1,3 mld dolarów (PKB tego kraju szacuje się na zaledwie 28 mld dolarów). Organizacja Narodów Zjednoczonych oszacowała natomiast, że za pomocą swoich operacji

i zakamuflowanemu cyberatakowi na system teleinformatyczny Komisji Nadzoru Finansowego (KNF) dokonanemu w Polsce w 2021 r. Chociaż wszystkie cele atakujących do dzisiaj nie są jawne, jednym z nich było przedostanie się do zaufanej sieci wewnętrznej systemów bankowych, przejęcie kontroli nad komputerami tam umieszczonymi i ustanowienie komunikacji pomiędzy systemami ofiary a infrastrukturą kontrolowaną przez przestępców[77].

Skuteczne działania przeciwko zorganizowanym grupom przestępczym operującym w Internecie wymagają tworzenia zespołów operacyjnych składających się z przedstawicieli różnych służb ochrony prawa, a nierzadko także podjęcia współpracy międzynarodowej. W Stanach Zjednoczonych powstała specjalna jednostka o nazwie J-CODE (ang. Joint Criminal Opioid and Darknet Enforcement) do walki z cyberprzestępcami, którą tworzy siedem instytucji, m.in. FBI, HSI, Departament Sprawiedliwości oraz Służba Kontroli Pocztowej (ang. The Postal Inspection Service). Wynika z tego, że trudna do przecenienia rola w zwalczaniu wirtualnego handlu substancjami zabronionymi przypada straży granicznej, inspekcji celnej i poczcie, gdyż realizacja usługi transportu towaru zamówionego przez Internet to moment, kiedy wirtualny świat przestępców styka się ze światem materialnym, a powstała w ten sposób sytuacja pozwala nie tylko przejąć nielegalny towar, lecz także podjąć inne działania pod kątem ustalenia i zatrzymania przestępców[78]. Niewskazany jest zatem stan rzeczy zaobserwowany w jednej z krajowych służb, w której odseparowano od siebie pion zajmujący się odzyskiwaniem mienia od komórek realizujących czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze. Efektywne zwalczanie przestępczości kryptowalutowej, w tym realizacja zabezpieczenia majątkowego na tokenach cyfrowych, wymaga stałej współpracy i szybkiego przepływu informacji pomiędzy osobami zajmującymi się różnymi aspektami zwalczania przestępstw, tj. pracą operacyjną, dochodzeniową, odzyskiwaniem mienia. *A contrario* osoba zajmująca się odzyskiwaniem majątku pochodzącego z przestępstwa będzie

cybernetycznych Korea Północna zgromadziła w 2019 r. ponad 2 mld dolarów pochodzących z nielegalnego finansowania w celu sfinansowania programu zbrojeniowego.

77 Więcej na temat ataku zob. A. Maciąg, I. Tarnowski, *Atak teleinformatyczny na polski sektor finansowy*, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 11 V 2023].

78 P. Opitek, *Biegły z zakresu kryptowalut w sprawach karnych*, w: *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, D. Zienkiewicz (red.), Toruń 2021, s. 434.

miała poważne trudności z realizacją tego zadania w stosunku do kryptoaktywów, jeśli w ogóle nie uczestniczy w czynnościach procesowych polegających na przeszukaniu czy przesłuchaniu świadka lub nie ma dostępu do bieżących informacji z ustaleń pozaprocesowych.

Ciekawie rysuje się problem stosowania kontroli operacyjnej w postaci uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych[79], a więc kontroli urządzenia końcowego. Można z całą pewnością stwierdzić, że dzisiaj walka z cyberprzestępczością wymaga stosowania takiej metody pracy operacyjnej, gdyż przestępcy kontaktują się ze sobą głównie za pomocą urządzeń tworzących sieć Internet. Prawo jednoznacznie dopuszcza uzyskiwanie danych zapisanych na dysku urządzenia jako jedną z form kontroli operacyjnej. Obecnie wysiłek Policji, jak również Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego, powinien skupiać się na zwiększaniu zdolności technicznych do kontroli operacyjnej pamięci laptopa, telefonu, modemu czy routera w sposób pasywny, tj. bez modyfikowania śladów cyfrowych znajdujących się w kontrolowanym przedmiocie. Idealnym rozwiązaniem byłoby objęcie kontrolą operacyjną sprzętowego portfela kryptowalutowego, chociaż pod względem technicznym jest to zadanie trudne do realizacji. Umożliwiłoby to m.in. poznanie całej historii transakcji, aktualnej wysokości salda bitcoinów znajdujących się w urządzeniu czy nawet realizację zabezpieczenia majątkowego na ujawnionych kryptowalutach[80]. Podobnych informacji dostarczyłoby objęcie kontrolą w formie uzyskiwania i utrwalania treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej, założonego na giełdzie konta tzw. figuranta, na które są przesyłane dodatkowe dane, jak chociażby kody do wypłat pieniędzy w bankomacie po konwersji krypto na pieniądz fiducjarny. Co prawda na podstawie pisma lub postanowienia prokuratora można żądać od administratora giełdy przedłożenia wspomnianych danych, ale przejęcie kontroli nad kontem pomogłoby w uzyskiwaniu na bieżąco informacji i planowaniu z wyprzedzeniem realizacji zadań. Patrząc szerzej,

[79] Taka metoda kontroli jest przewidziana w ustawach regulujących pracę Policji i 9 służb.

[80] Stwierdzenie, że w portfelu znajdują się jednostki waluty wirtualnej, stanowi skrót myślowy. W rzeczywistości bowiem portfel zawiera dane cyfrowe umożliwiające zarządzanie jednostkami altcoinów w postaci tzw. klucza publicznego i prywatnego, ale same tokeny są odwzorowane w księdze rozrachunkowej nazywanej blockchainem w formie cyfrowego zapisu danych.

zasadne jest wprowadzenie nowej metody kontroli operacyjnej w postaci nieprzerwanego („w locie") śledzenia transferów pieniądza bezgotówkowego, innych środków płatniczych lub kryptoaktywów poprzez ustanowienie nowej, ustawowej formy pracy operacyjnej[81].

W zwalczaniu przestępczości kryptowalutowej znajdują zastosowanie tradycyjne metody i formy pracy operacyjnej. Na przykład funkcjonariusz Policji czy służby specjalnej operujący na platformie internetowej pod legendą jej rzeczywistego użytkownika otrzymuje status FPP, tj. funkcjonariusza działającego pod przykryciem, ze wszystkimi tego konsekwencjami. Dochodzi zatem do realizacji kombinacji operacyjnej w postaci np. zakupu kontrolowanego narkotyków przez agenta, a następnie przesyłki niejawnie nadzorowanej. Ma to na celu rozpracowanie środowiska osób uczestniczących w handlu internetowym nielegalnymi substancjami, ustalenia sposobu przesyłania narkotyków i dostarczania ich klientowi, składu chemicznego tych substancji oraz sposobu komunikowania się pomiędzy kupującym i sprzedającym. Kryptowaluty przeznaczone do płatności za założenie konta czy uiszczenia ceny towaru będą pochodzić z funduszu operacyjnego służby, a operacje nimi dokonywane są szczegółowo dokumentowane aż do pełnego rozliczenia kosztów podjętych działań. Muszą być one odpowiednio dokumentowane w formie notatek z przeprowadzonych czynności na każdym etapie operacji specjalnej wraz z dołączonymi zdjęciami ekranu, a najlepiej nagraniem wideo, dokumentującymi to, co FPP wykonuje w cyberprzestrzeni. Ważne są zrzuty rozmów na komunikatorach prowadzonych przez agenta z osobami łamiącymi prawo, gdyż najczęściej w takiej formie cyberprzestępcy przekazują sobie informacje. Dokumenty z przeprowadzonych czynności, stanowiące materiał dowodowy świadczący o podejrzeniu popełnienia przestępstwa, powinny być w odpowiednim momencie udostępnione przez komendanta Policji lub szefa służby specjalnej do postępowania karnego.

Śledztwo dotyczące przestępczości kryptowalutowej

Rok 2022 był rekordowy pod względem liczby szkoleń i konferencji na temat walut wirtualnych zorganizowanych przez polskie organy ścigania.

[81] Szerzej na ten temat zob. P. Opitek, *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)*, „Prokuratura i Prawo" 2021, nr 2, s. 154–175.

Najwięcej uwagi poświęcono tematowi zabezpieczenia majątkowego na kryptowalutach. Okazuje się jednak, że stricte procesowa realizacja samego zabezpieczenia (tj. wydanie stosownych decyzji przez prokuratora) jest łatwiejsza niż ujawnienie bitcoinów pochodzących z przestępstwa i faktyczne objęcie ich w posiadanie samoistne. Śledztwo dotyczące przestępczości kryptowalutowej w sprawach o dużym ciężarze gatunkowym lub takich, w których istnieje realna możliwość postawienia konkretnych osób w stan oskarżenia, to żmudny proces wykrywczy związany z gromadzeniem obszernego materiału dowodowego. Sukces tego śledztwa zależy od wiedzy i determinacji osób je prowadzących, a niekiedy decyduje o nim również łut szczęścia.

Omawiane postępowania karne wymagają posiadania umiejętności w zakresie gromadzenia śladów cyfrowych oraz dowodów nie tylko od polskich i zagranicznych dostawców usług sieciowych, takich jak giełdy i kantory kryptowalutowe, lecz także od przedsiębiorców dostarczających Internet, operatorów telekomunikacyjnych czy instytucji finansowych, na czele z bankami. Wiadomości cenne dla postępowania przygotowawczego mogą mieć także administratorzy systemów monitoringu przemysłowego (nagrania wypłat bankomatowych), zarządcy dróg krajowych (rejestracja przemieszczania się pojazdów), przewoźnicy w transporcie samolotowym, podmioty obsługujące szybkie płatności typu BLIK czy administratorzy platform handlowych w sieci. Niemniej jednak źródłem największej ilości danych nadal pozostają giełdy kryptowalutowe. Można zażądać od nich wydania informacji dotyczących:

- danych osobowych użytkownika giełdy, które są gromadzone w trakcie realizacji procedury KYC i mogą być zmieniane w trakcie korzystania przez klienta z platformy (imię, nazwisko, data urodzenia, PESEL, numer telefonu, adres zamieszkania itd.);
- skanu dokumentów potwierdzających jego tożsamość (dowód osobisty, prawo jazdy, paszport itp.) oraz innych dokumentów przedłożonych przez klienta w trakcie korzystania z usług oferowanych przez giełdę (np. deklaracji o źródle pochodzenia inwestowanych środków);
- informacji o zrealizowanych transakcjach w walutach wirtualnych i pieniądzu fiducjarnym (wykaz transakcji, ich data, wartość operacji, beneficjent otrzymanych środków);
- daty dostępu do systemu giełdy przez potencjalnego sprawcę (przedłożenie zestawienia logowań do platformy osób pozostających

w zainteresowaniu organów ścigania, wraz z wszelkimi atrybutami w postaci adresów IP portów ze wskazaniem dokładnego czasu logowania, lokalizacji BTS, numerów IMEI/MAC urządzenia inicjującego połączenia internetowe). Należy ponadto sprawdzić, czy dodano nowe urządzenie zaufane do logowań na konto giełdy oraz dane urządzeń, z których następowały logowania (system operacyjny, wersja systemu, rozdzielczość ekranu, wersja przeglądarki);
- historii konta użytkownika giełdy (kody wysłane do przeprowadzenia transakcji bankomatowych, informacje i ostrzeżenia otrzymane od administratora giełdy);
- informacji, czy w trakcie trwania stosunków gospodarczych z klientem wystąpiły anomalie transakcyjne (np. transakcja została niezrealizowana, gdyż środki pochodziły z adresu uznanego za podejrzany, blokowano rachunki bankowe lub adresy walut wirtualnych, wstrzymywano transakcje – jeśli tak, to kiedy i dlaczego);
- zapisów rozmów telefonicznych lub wideokonferencji przeprowadzonych pomiędzy pracownikami giełdy a osobą podejrzewaną;
- dokonywania przez instytucję obowiązaną zgłoszenia do GIIF, prokuratury lub innego organu publicznego w sprawie użytkownika giełdy (kiedy i z jakiego powodu wystosowano zgłoszenie);
- wypłat „skradzionych" środków, zwłaszcza docelowego adresu portfela, na który wypłacono środki, oraz identyfikatora transakcji (*hash* transakcji).

Procedury i zakres danych (np. logi) oraz informacji (historia transakcji) możliwych do uzyskania od giełd zależą od kilku czynników, m.in. siedziby giełdy, rodzaju i ilości danych pozostawionych na platformie przez jej użytkownika czy etapu postępowania karnego. Organy ścigania i dostarczyciele usług sieciowych wypracowali wiele zasad współpracy. Niekiedy otrzymanie żądanych przez prokuratora treści jest realizowane na podstawie pisma procesowego. Wniosek powinien wskazywać funkcjonariusza i jednostkę prowadzącą sprawę, sygnaturę postępowania, zawierać krótki opis sprawy ze wskazaniem, jakie przestępstwo zarzuca się osobie, której dotyczy wniosek. Należy przesłać go drogą elektroniczną na adres oficjalnego punktu kontaktowego giełdy, o którym informację posiadają zazwyczaj organy ochrony prawa. Pismo powinno być sporządzone w języku angielskim lub języku kraju, w którym funkcjonuje giełda. Dokument główny powinien stanowić skan pisma urzędowego, a załącznik ze szczegółowymi danymi należy wysłać w formie edytowalnej po to, aby było możliwe

skopiowanie danych (np. adresów kryptowalutowych) i dalsza praca na nich. Jeśli sprawa ma charakter pilny, to należy to w piśmie wyraźnie zaznaczyć. Co ważne, ponieważ niektóre giełdy informują swoich klientów o prowadzonym w stosunku do nich śledztwie, to we wniosku można zastrzec, aby dostarczyciel usług sieciowych zaniechał takiego poinformowania, oraz uzasadnić to żądanie.

Są jednak jurysdykcje, w których uzyskanie informacji innych niż metadane (ang. *non-content data*) będzie uwarunkowane wydaniem nakazu przez właściwy miejscowo sąd. Wówczas wnioski o międzynarodową pomoc prawną są kierowane na podstawie umów zawieranych między suwerennymi państwami, co w praktyce znacznie wydłuża proces gromadzenia artefaktów. Dotyczy to m.in. Stanów Zjednoczonych, a więc terytorium, na którym funkcjonuje największa liczba firm będących dostarczycielami usług sieciowych. W Europie pomocny okazuje się europejski nakaz dochodzeniowy powszechnie stosowany przez funkcjonariuszy policji i prokuratorów. Osoba zajmująca się przestępczością kryptowalutową musi zatem orientować się zarówno w prawnych, jak i praktycznych aspektach uzyskiwania dowodów, gdyż procedura z tym związana zależy od kilku czynników:

- siedziby firmy oraz usytuowania serwera z danymi;
- rodzaju danych, o które chodzi: *content data* czy *non-content data* (te ostatnie często są udostępniane w sposób odformalizowany);
- zastosowanej procedury: „zamrażania" danych do czasu uzyskania zezwolenia na ich przekazanie, procedury uzyskania właściwych danych czy pilnego uzyskiwania danych w sytuacjach nadzwyczajnych (ang. *emergency cases*);
- polityki wewnętrznej podmiotu zobowiązanego do udostępniania informacji i danych w zakresie zarządzania nimi.

Ostatecznie, jeśli giełda lub inna platforma cyfrowa odmawia realizacji przewidzianej przez prawo procedury wydania danych i informacji lub znacznie ją utrudnia, można rozważyć zajęcie jej serwera w celu ekstrakcji niezbędnych artefaktów lub sprawdzenia, czy nie zostały z niego usunięte. Czasami wizja nieuchronności zajęcia infrastruktury prowadzi do otwarcia się na współpracę ze strony dostawcy usług. Takie działania są niemożliwe w stosunku do podmiotów działających w darkmarkecie, w którym lokalizacja ich infrastruktury jest nieznana, oraz w krajach niewspółpracujących w ramach międzynarodowej pomocy prawnej.

Kolejne ważne informacje dla śledztwa z wątkiem kryptowalutowym są zapisane na sprzęcie elektronicznym wykorzystywanym przez

użytkowników końcowych protokołu Bitcoina, a przede wszystkim w ich telefonach i komputerach. Na zabezpieczonym dowodowym nośniku danych znajdują się artefakty pozwalające ustalić, czy jego użytkownik posługiwał się walutami wirtualnymi, łączył się ze stronami przeznaczonymi do ich obsługi, a w pamięci komputera, w tym operacyjnej RAM, mogą znajdować się ślady lub informacje (hasła, loginy itp.) pozwalające autoryzować dostęp do baz danych, tj. aplikacji, zasobów chmurowych czy portfela kryptowalutowego. Jeśli w jakimkolwiek systemie ujawniono dane statuujące tokeny cyfrowe i należące do podejrzanego, to trzeba je niezwłocznie zabezpieczyć na potrzeby toczącego się śledztwa. W tym celu autorzy postulują, aby utworzyć w jednej z wiodących służb specjalnych w obszarze bezpieczeństwa ekonomicznego RP (np. ABW) lub Policji grupę operacyjno-śledczą składającą się z funkcjonariuszy, którzy będą mieli kompetencje związane z zabezpieczaniem bitcoinów i posiadali zaplecze technologiczne do ich przejmowania we władanie. Chodzi o takie umiejętności, jak oględziny lub przeszukanie systemu informatycznego komputera stanowiącego dowód w miejscu jego ujawnienia, obsługa elektronicznej portmonetki należącej do sprawców czynu zabronionego, ale także o dysponowanie przez formacje zwalczające przestępstwa własnym portfelem sprzętowym do przyjmowania kryptowaluty, rozpoznawania rodzajów cyfrowych aktywów, generowania dla nich adresów. Szczególnie ważna jest instytucja zabezpieczenia majątkowego na kryptowalutach, o której mowa w art. 291 § 1 k.p.k. i nast. W Polsce takie zabezpieczenia są realizowane od kilku już lat (pierwsze wykonano w 2017 r.), a z każdym rokiem ich liczba rośnie. W celu przejęcia bitcoinów funkcjonariusze Policji najczęściej współpracowali z internetowymi giełdami, które najpierw zamrażały środki znajdujące się na podejrzanym koncie, a następnie tworzyły specjalne konto dla prokuratury i na nim składowały przedmiot zabezpieczenia. Znany jest także co najmniej jeden przypadek wygenerowania przez policjantów portfela papierowego, ale najbardziej bezpieczne i praktyczne jest dysponowanie przez służby portfelem sprzętowym typu Ledger lub Trezor. Najtrudniejszym zadaniem w toku czynności operacyjno-rozpoznawczych lub dochodzeniowo-śledczych wydaje się ustalenie, gdzie znajdują się waluty wirtualne pochodzące ze śledztwa, a następnie uzyskanie do nich faktycznego dostępu z możliwością transferu na adres zarządzany przez prowadzącego postępowanie. Znane są bowiem przypadki, w których na podstawie analizy kryminalnej transferów kryptowalutowych ustalono adresy składowania znacznych ilości tokenów pochodzących z przestępstwa,

np. włamań na giełdy, ale nie były one powiązane z żadną z publicznych platform internetowych, brakowało ustaleń w zakresie osób zarządzających tymi adresami i w konsekwencji – możliwości przejęcia władztwa nad środkami wirtualnymi. W takiej sytuacji pozostaje tylko oflagowanie takiego adresu, a więc jego monitorowanie w oczekiwaniu, aż zgromadzone na nim środki zostaną przez kogoś przelane na inny, mniej anonimowy adres.

W przypadku bitcoinów, które zostały już przejęte przez organy ścigania, pojawiają się trudności prawne i faktyczne z ich przechowywaniem. Wynikają one z tego, że cena walut wirtualnych jest bardzo płynna i podlega dużym różnicom kursowym w krótkich odstępach czasu, a każdy z portfeli jest narażony na atak hakerski, uszkodzenie mechaniczne lub informatyczne, a ponadto może zdarzyć się błąd ludzki związany z ich obsługą. Ponadto polskie sądy nie są gotowe na przejmowanie kryptowalut, które zostałyby przekazane wraz z aktem oskarżenia. Praktycznym rozwiązaniem tych problemów jest sprzedaż zabezpieczonego majątku w trakcie śledztwa na podstawie art. 232 § 1 k.p.k. w zw. z art. 236a k.p.k. Stanowią one, że przedmioty, których przechowywanie byłoby połączone z nadmiernymi trudnościami albo powodowałoby znaczne obniżenie wartości rzeczy, można sprzedać według trybu określonego dla właściwych organów postępowania wykonawczego, a ten przepis stosuje się odpowiednio do tokenów cyfrowych stanowiących dane informatyczne. Sprzedaż rzeczy następuje według przepisów o postępowaniu egzekucyjnym w administracji lub zawartych w Kodeksie postępowania cywilnego w zależności od tego, jaka była podstawa zajęcia środków (art. 291 § 1 pkt 1–5 k.p.k.). Inny problem prawny dotyczy treści art. 295 § 1 k.p.k., w którym jest mowa o mieniu ruchomym, a bitcoin nie jest rzeczą w rozumieniu art. 45 k.c. W praktyce jednak instytucja tymczasowego zajęcia mienia ruchomego była już efektywnie stosowana w odniesieniu do walut wirtualnych, a ponadto rozwiązaniem w takim przypadku może okazać się art. 236b k.p.k., a więc uznanie kryptowaluty za środki zgromadzone na rachunku i wydanie postanowienia w przedmiocie dowodów rzeczowych.

Ślady cyfrowe dotyczące walut wirtualnych oraz – ogólniej rzecz biorąc – popełnionego cyberprzestępstwa należy odpowiednio gromadzić, zabezpieczać, a następnie wykorzystywać w śledztwie. Prezentacja w toku postępowania karnego dowodu cyfrowego opiera się na regule, że stanowi on nie tylko to, co widać, lecz także ma metadane. Problem ten zaistniał we wspomnianej już w artykule sprawie rozpatrywanej przed Sądem Rejonowym w Przasnyszu, w której prokurator jako dowód

na wygląd i sposób funkcjonowania stron internetowych poświęconych skinom załączył do aktu oskarżenia wydruki takich stron. W piśmie procesowym obrońca oskarżonego wskazał nieprzydatność dowodu w postaci papierowych wydruków stron internetowych, na których znajdowały się informacje stanowiące – zdaniem oskarżyciela publicznego – dowód popełnienia przestępstwa zarzucanego oskarżonemu. Obrońca oskarżonego podniósł, że:

> (...) w analizowanym stanie faktycznym ewidentnie ma miejsce sytuacja, polegająca na tym, że przeprowadzenie dowodu wskazanego we wniosku dowodowym nie może doprowadzić do stwierdzenia okoliczności w nim wskazanej. Strona internetowa ma charakter interaktywny i sam tylko 'zrzut ekranu' i do tego wydrukowany na kartce papieru nie oddaje jej istoty i sposobu funkcjonowania. Zdaniem obrońcy dowód na okoliczności, których dotyczą zakwestionowane wydruki stron internetowych, powinny zostać przeprowadzone w ten sposób, że oskarżyciel, podczas postępowania dowodowego, odtworzy funkcjonowanie ustalonych stron internetowych. Jest to z całą pewnością technicznie możliwe (chociażby poprzez zapisanie stron na trwały nośnik), ale niewątpliwie wymaga od oskarżyciela nieco więcej wysiłku[82].

Sąd podzielił stanowisko obrony, a to, a także z uwagi na wiele innych błędów popełnionych podczas dochodzenia, skutkowało uniewinnieniem oskarżonego. Wynika z tego, że funkcjonariusze służb powinni mieć wiedzę, umiejętności i należyte oprogramowanie do interaktywnych oględzin lub przeszukiwania stron internetowych[83]. Szczególnie ta druga czynność, tj. przeszukanie w cyberprzestrzeni, mogłaby być częściej wykonywana w toku czynności procesowych, gdyż pozwala uzyskać informacje i zabezpieczyć najważniejsze dowody dla śledztwa, a mimo to referenci spraw karnych albo obawiają się realizacji takich, ich zdaniem, trudnych czynności, albo robią to bez należytej staranności w postaci sporządzenia notatki urzędowej, pomimo że art. 143 § 1 pkt 1 i 6 k.p.k. wymaga w tym przypadku spisania protokołu.

[82] Akta sprawy Sądu Rejonowego w Przasnyszu II Wydział Karny, sygn. akt II K 608/18.

[83] Zob. P. Opitek, *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, „Prokuratura i Prawo" 2022, nr 9, s. 100–128.

Wnioski końcowe

Przeprowadzona analiza wybranych aspektów przestępczości z wykorzystaniem walut wirtualnych prowadzi do kilku podstawowych wniosków. Rola kryptoaktywów w działalności profesjonalnych podmiotów rynku kapitałowego stale rośnie i coraz więcej osób użytkuje tego rodzaju mienie. Kryptoaluty są wykorzystywane także przez przestępców, a liczba spraw karnych związanych przestępczością kryptowalutową z każdym rokiem wzrasta. Raporty instytucji publicznych i doświadczenia autorów pokazują, że nielegalne działania z udziałem infrastruktury krypto mogą dotyczyć poważnych czynów karalnych godzących w podstawy ekonomiczne państwa, służyć do sponsorowania terroryzmu i działań szpiegowskich, korupcji, omijania sankcji, a zatem wpływać na bezpieczeństwo Polski i jej renomę na arenie międzynarodowej. Prowadzi to do prostego wniosku, że organy ścigania, w tym odpowiednie służby specjalne, muszą dysponować wielowymiarowymi zdolnościami (odpowiednio przygotowanymi ludźmi i zapleczem logistycznym) do pracy z kryptowalutami, w kwestiiach zarówno ogólnych (praca z dowodami cyfrowymi, poznanie istoty technologii blockchain), jak i szczegółowych (umiejętność posługiwania się wirtualnymi portfelami, redefinicja pracy funkcjonariusza pod przykryciem w cyberprzestrzeni, a być może stworzenie funduszu operacyjnego w postaci kryptoaktywów). Oczywiste jest, że nie każdy funkcjonariusz takiej instytucji będzie specjalistą w zakresie kryptowalut, niemniej powinien on bezzwłocznie otrzymać profesjonalne wsparcie w momencie, gdy w jego postępowaniu zaistnieją tematy związane z tokenami cyfrowymi. Biorąc ponadto pod uwagę, że nie zawsze jest możliwa współpraca lidera ochrony bezpieczeństwa państwa z innymi organami ochrony prawa wyspecjalizowanymi w zwalczaniu cyberprzestępczości, to tym bardziej tak elitarna formacja powinna mieć własną grupę (strukturę) osób wyspecjalizowanych w realizacji czynności procesowych i pozaprocesowych dotyczących kryptowalut (np. zabezpieczenia majątkowego na bitcoinie).

Patrząc szerzej, należy monitorować polski rynek walut wirtualnych pod kątem ewentualnego prania pieniędzy z wykorzystaniem wartości binarnych czy omijania sankcji nałożonych na Białoruś i Rosję. Instrumenty przydatne do realizacji wspomnianych zadań oferuje u.p.p.p. Wszystkich celów dotyczących minimalizowania zagrożeń bazujących na kryptoaktywach nie sposób osiągnąć bez instytucjonalnej współpracy pomiędzy ABW, prokuraturą, GIIF i KNF, gdyż każda z tych instytucji ma swoiste, tylko jej

przypisane narzędzia prawne i możliwości faktyczne. Dopiero ich synergia daje możliwość budowy skutecznej i wszechstronnej polityki AML/CFT.

Analiza tematu kryptowalut pokazała, że zostały one użyte także do wspierania działań terrorystycznych o różnym charakterze – sponsorowania organizacji terrorystycznych z wykorzystaniem internetowego crowdfundingu, bezpośrednich dotacji na rzecz konkretnej osoby pomagającej w organizacji zamachów lub motywowanej do nich czy też cyberataków ukierunkowanych na infrastrukturę teleinformatyczną obszarów kluczowych dla funkcjonowania państwa. Z informacji podanych przez przedstawiciela HSI wynika, że w Stanach Zjednoczonych liczba postępowań karnych dotyczących kryptowalut wzrosła od jednego w 2011 r. do ponad 604 śledztw w 2021 r. Przez ten czas HSI skonfiskowała bitcoiny i altcoiny o równowartości 79 825 606,65 dolarów. Obrazuje to rosnące zaufanie sprawców czynów nielegalnych o najwyższym ciężarze gatunkowym do kryptoaktywów, a zatem implikuje konieczność zdobywania przez organy ścigania kompetencji do walki z tym rodzajem finansowania terroryzmu[84]. I chociaż główne źródła tego finansowania nadal opierają się na tradycyjnych instytucjach finansowych[85] (szacuje się, że obecnie finansowanie terroryzmu za pomocą kryptowalut generuje tylko 1% takich transakcji[86]), to problem z pewnością będzie narastał. Sposoby działania i podejście sprawców do świata wirtualnego zmieniają się i ewoluują ku najkorzystniejszym dla nich rozwiązaniom. Dzięki opisanym w artykule skutecznym akcjom amerykańskich służb przeciwko platformom internetowym Brygady Izz ad-Din al-Kassam w kwietniu 2023 r. oświadczyło, że zawiesza zbieranie datków z wykorzystaniem bitcoina, powołując się na wzrost „wrogiej" działalności wobec darczyńców. *Wynika to z troski o bezpieczeństwo darczyńców i chęci oszczędzenia im wszelkich szykan* – brzmiał komunikat Hamasu[87]. Jednocześnie wezwano do (...) *kontynuowania darowizn na rzecz Kassama i ruchu oporu wszelkimi dostępnymi środkami*[88].

[84] *Statement of John Eisert...*, s. 14–16.

[85] *Risk Assessment. 2022 National Terrorist Financing...*

[86] *Statement of Ranking Member August Pfluger*, w: *Terrorism and Digital Financing...*, s. 3.

[87] N. Al-Mughrabi, *Hamas armed wing announces suspension of bitcoin fundraising*, Reuters, 28 IV 2023 r., https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ [dostęp: 9 V 2023]; *Hamas armed wing to stop crypto fundraising over 'hostility' against donors*, i24NEWS, 30 IV 2023 r., https://www.i24news.tv/en/news/middle-east/palestinian-territories/1682688395-hamas-armed-wing-to-stop-crypto-fundraising-citing-hostility-against-donors [dostęp: 9 V 2023].

[88] Tamże.

Polska jest podmiotem działań terrorystycznych wykorzystujących infrastrukturę Internetu i kryptowaluty. Są to m.in. wymierzone w RP ataki ransomware czy zamieszczone w Darknecie, operującym bitcoinem, ogłoszenia zachęcające do zabójstw najważniejszych, wymienionych z imienia i nazwiska, polskich polityków. Zagadnienia dotyczące kryptowalut są powiązane także z działalnością wrogich organizacji wywiadowczych ukierunkowaną na bezpieczeństwo Polski. Konieczne jest zatem, aby najważniejsze służby ochrony państwa zwiększały swoje kompetencje w zakresie aktywności w świecie wirtualnym, realizacji cyberoperacji i przeciwdziałania wrogim atakom IT. Dotyczy to m.in. umiejętności badania transferów kryptowalutowych, zabezpieczania takich wartości majątkowych, ale także ich wykorzystywania do realizacji własnych celów.

Bibliografia

Chainalysis, *The 2022 Crypto Crime Report*, luty 2022 r.

Ocieczek G., Opitek P., *Analiza definicji walut wirtualnych z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Consilium Iuridicum" 2022, nr 3–4, s. 122–139.

Opitek P., *Biegły z zakresu kryptowalut w sprawach karnych*, w: *Wokół kryminalistyki. Nauka i praktyka. Księga pamiątkowa dedykowana Profesorowi Tadeuszowi Widle*, D. Zienkiewicz (red.), Toruń 2021, s. 413–447.

Opitek P., *Funkcjonowanie instrumentów finansowych w oparciu o technologię blockchain*, Łódź 2022.

Opitek P., *Kontrola transferów pieniądza bezgotówkowego w czasie rzeczywistym jako nowa forma czynności operacyjno-rozpoznawczych na przykładzie ustawy o Agencji Bezpieczeństwa Wewnętrznego (postulaty de lege ferenda)*, „Prokuratura i Prawo" 2021, nr 2, s. 154–175.

Opitek P., *Kryptowaluty w aspekcie czynności dochodzeniowo-śledczych Policji*, „Przegląd Policyjny" 2017, nr 2, s. 138–158. https://doi.org/10.5604/01.3001.0013.6082.

Opitek P., *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 41–70, Lex, https://sip.lex.pl/komentarze-i-publikacje/artykuly/przeciwdzialanie-praniu-pieniedzy-z-wykorzystaniem-walut-151383722.

Opitek P., *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, „Prokuratura i Prawo" 2022, nr 9, s. 100–128.

Opitek P., *Wykorzystanie walut i serwisów wirtualnych do prania pieniędzy i finasowania terroryzmu*, Warszawa 2019 (praca dyplomowa napisana na studiach podyplomowych w Szkole Głównej Handlowej, niepublikowana, w zasobach autora).

Prawo cywilne – część ogólna, M. Safjan (red.), seria: System Prawa Prywatnego, t. 1, Warszawa 2007.

Przewłoka E., *Metodyka podstawowych czynności realizowanych przez funkcjonariusza Policji i związanych z przestępstwem „kradzieży" waluty wirtualnej*, Bydgoszcz 2023 (metodyka wewnętrzna Policji, w zbiorach autora).

Skała J., *Uzyskiwanie przez prokuratora informacji i danych od instytucji obowiązanych na podstawie ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, z. 3, s. 83–100. https://doi.org/10.53024/4.3.47.2022.

Źródła internetowe

Al-Mughrabi N., *Hamas armed wing announces suspension of bitcoin fundraising*, Reuters, 28 IV 2023 r., https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/ [dostęp: 9 V 2023]

Alnasaa M. i in., *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*, International Monetary Fund, 25 III 2022 r., https://www.imf.org/en/Publications/WP/Issues/2022/03/25/Crypto-Corruption-and-Capital-Controls-Cross-Country-Correlations-515676 [dostęp: 4 V 2023].

Anti-money laundering: Provisional agreement reached on transparency of crypto asset transfers, Council of the EU, 29 VI 2022 r., https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/ [dostęp: 7 IV 2023].

Berton B., *The dark side of the web: ISIL's one-stop shop?*, European Union Institute for Security Studies, czerwiec 2015 r., https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [dostęp: 23 VIII 2019].

Bitcoin wa Sadaqat al-Jihad, https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf [dostęp: 20 I 2019].

CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange, CFTC, 27 III 2023 r., https://www.cftc.gov/PressRoom/PressReleases/8680-23 [dostęp: 9 IV 2023].

Crypto-assets. Relevant provision: Article 5b(2) of Council regulation (EU) NO 833/2014, https://finance.ec.europa.eu/system/files/2023-03/faqs-sanctions-russia-crypto_en.pdf [dostęp: 10 IV 2023].

Crypto exchanges Huobi, KuCoin enabled Russian sanction evasion. Binance also mentioned, Ledger Insights, 28 II 2023 r., https://www.ledgerinsights.com/russia-sanctions-crypto-exchanges-huobi-kucoin-binance/ [dostęp: 10 IV 2023].

Dugas M., *The Latest North Korea Cyber Indictment Should Serve as a Model*, Just Security, 24 II 2021 r., https://www.justsecurity.org/74930/the-latest-north-korea-cyber-indictment-should-serve-as-a-model/ [dostęp: 11 V 2023].

Farah D., Richardson M., *The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America*, Georgetown University, 20 III 2023 r., https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/ [dostęp: 6 IV 2023].

Fight against money laundering and terrorist financing, European Council, https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/ [dostęp: 9 IV 2023].

Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme, United States Attorney's Office, Eastern District of New York, 19 X 2022 r., https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money [dostęp: 7 IV 2023].

Germany and Ukraine hit two high-value ransomware targets, Europol, https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets [dostęp: 6 IV 2023].

Global Disruption of Three Terror Finance Cyber-Enabled Campaigns, The United States Department of Justice, 13 VIII 2020 r., https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns [dostęp: 9 V 2023].

Hamas armed wing to stop crypto fundraising over 'hostility' against donors, i24NEWS, 30 IV 2023 r., https://www.i24news.tv/en/news/middle-east/palestinian-territories/1682688395-hamas-armed-wing-to-stop-crypto-fundraising-citing-hostility-against-donors [dostęp: 9 V 2023].

How Russians Use Tether to Evade Global Sanctions, Inca Digital, https://inca.digital/intelligence/how-russians-use-tether/ [dostęp: 10 IV 2023].

https://counterstrike.fandom.com/wiki/Skins [dostęp: 17 II 2022].

Illicit Finance Risk Assessment of Decentralized Finance, U.S. Department of the Treasury, kwiecień 2023 r., https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [dostęp: 14 IV 2023].

Living on the Edge, International Monetary Fund, październik 2022 r., https://www.imf.org/en/Publications/REO/SSA/Issues/2022/10/14/regional-economic-outlook-for-sub-saharan-africa-october-2022 [dostęp: 5 IV 2023].

Maciąg A., Tarnowski I., *Atak teleinformatyczny na polski sektor finansowy,* Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/atak-teleinformatyczny-na-polski-sektor-finansowy/ [dostęp: 11 V 2023].

MUFG's Progmat security token platform to become digital asset joint venture, Ledger Insights, 7 X 2021 r., https://www.ledgerinsights.com/mufg-progmat-security-token-digital-asset-joint-venture/ [dostęp: 5 IV 2023].

MUFG, SBI share roadmap for Japanese security tokens, Ledger Insights, 7 X 2021 r., https://www.ledgerinsights.com/mufg-sbi-share-roadmap-for-japanese-security-token-platform/ [dostęp: 27 III 2023].

National Strategy for Combating Terrorist and Other Illicit Financing 2020, https://home.treasury.gov/system/files/136/National-Strategy-to-Counter-Illicit-Financev2.pdf [dostęp: 7 VII 2023].

O'Sullivan F., *Where Is Crypto Illegal in 2023? The Countries That Ban Cryptocurrency,* Cloudwards, 22 II 2023 r., https://www.cloudwards.net/where-is-crypto-illegal/ [dostęp: 5 IV 2023].

Perez Y.B., *Bitcoin, Paris and Terrorism: What the Media Got Wrong,* CoinDesk, 6 III 2023 r., https://www.coindesk.com/bitcoin-paris-and-terrorism-what-the-media-got-wrong [dostęp: 10 V 2023].

Preiss I., *Crypto AML rules passed by MEPs,* The Block, 28 III 2023 r., https://www.theblock.co/post/223215/crypto-aml-rules-passed-meps [dostęp: 6 IV 2023].

Ransomware Attacks on Critical Infrastructure Sectors, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/2022-09/Ransomware%20Attacks%20.pdf [dostęp: 11 V 2023].

Risk Assessment. 2022 National Terrorist Financing, Department of the Treasury, luty 2022 r., https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf [dostęp: 10 V 2023].

SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings, U.S. Securities and Exchange Commission, https://www.sec.gov/news/press-release/2021-145 [dostęp: 24 III 2023].

Sigalos M., Goswami R., *Sam Bankman-Fried paid over $40 million to bribe at least one official in China, DOJ alleges in new indictment*, CNBC, 28 III 2023 r., https://www.cnbc.com/2023/03/28/sam-bankman-fried-paid-over-40-million-to-bribe-at-least-one-chinese-official-doj-alleges-in-new-indictment.html [dostęp: 9 IV 2023].

Sutton S., Seligman L., *Two major crypto exchanges failed to block sanctioned Russians*, Politico, 24 II 2023 r., https://www.politico.com/news/2023/02/24/two-major-crypto-exchanges-failed-to-block-sanctioned-russians-00084391 [dostęp: 10 IV 2023].

Terrorism and Digital Financing: How Technology is Changing the Threat. Hearing before the Subcommittee on Intelligence and Counterterrorism of the Committee On Homeland Security House of Representatives, https://www.congress.gov/117/chrg/CHRG-117hhrg45867/CHRG-117hhrg45867.pdf [dostęp: 10 V 2023].

UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf [dostęp: 9 IV 2023].

United States of America v. Samuel Bankman-Fried, https://storage.courtlistener.com/recap/gov.uscourts.nysd.590940/gov.uscourts.nysd.590940.80.0.pdf [dostęp: 7 IV 2023].

United States of America v. Ali Shukri Amin, CRIMINAL NO. 1:15-CR-164, https://www.investigativeproject.org/documents/case_docs/2826.pdf [dostęp: 10 V 2023].

Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, FATF, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html [dostęp: 7 IV 2023].

White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets, The White House, 16 IX 2022 r., https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/ [dostęp: 9 IV 2023].

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Dz. Urz. UE L 156/43 z 19 VI 2018 r.).

Rozporządzenie Rady (UE) NR 833/2014 z dnia 31 lipca 2014 r. dotyczące środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE L 229/1 z 31 VII 2014 r.).

Ustawa z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw (DzU z 2021 r. poz. 815, ze zm.).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. DzU z 2023 r. poz. 1124, ze zm.).

Ustawa z dnia 19 listopada 2009 r. o grach hazardowych (t.j. DzU z 2023 r. poz. 227).

Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. DzU z 2023 r. poz. 172, z 2022 r. poz. 2600).

Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy (t.j. DzU z 2023 r. poz. 654, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. DzU z 2022 r. poz. 1138, ze zm.).

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. DzU z 2022 r. poz. 1360, ze zm.).

Ensuring Responsible Development of Digital Assets, Executive Order 14067 of March 9, 2022, Federal Register. The Daily Journal of the United States Government, https://www.federalregister.gov/documents/2022/03/14/2022-05471/ensuring-responsible-development-of-digital-assets [dostęp: 5 IV 2023].

Orzecznictwo

Akta sprawy Sądu Rejonowego w Przasnyszu II Wydział Karny, sygn. akt II K 608/18.

Wyrok Sądu Okręgowego w Ostrołęce z 27 VIII 2020 r., sygn. akt II Ka 40/20.

Wyrok Sądu Rejonowego dla Krakowa-Krowodrzy II Wydział Karny z 3 VIII 2012 r., sygn. akt II Ka 776/11/K.

Inne dokumenty

Markets in crypto-assets (MiCA), https://www.europarl.europa.eu [dostęp: 9 IV 2023].
Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593 [dostęp: 9 IV 2023].

Poglądy zawarte w artykule są osobistymi poglądami autorów i nie wyrażają oficjalnego stanowiska instytucji, w której są zatrudnieni.

Dr Paweł Opitek

Doktor nauk prawnych, prokurator Prokuratury Okręgowej w Krakowie delegowany do Prokuratury Krajowej.

Dr Agnieszka Butor-Keler

Doktor w dziedzinie nauk społecznych w dyscyplinie ekonomia i finanse, adiunkt w Katedrze Rachunkowości Menedżerskiej w Szkole Głównej Handlowej w Warszawie.

Karol Kanclerz

Aplikant radcowski, główny specjalista w Departamencie Prawnym Urzędu Komisji Nadzoru Finansowego.