Ius Novum

2023, vol. 17, nr 4, s. 16–39

# WSPÓŁPRACA Z KRAJAMI TRZECIMI W ZWALCZANIU PRANIA PIENIĘDZY W OBLICZU WSPÓŁCZESNYCH WYZWAŃ

ANNA GOLONKA*

DOI: 10.26399/iusnovum.v17.4.2023.27/a.golonka

Streszczenie

Opracowanie poświęcono problematyce współpracy międzynarodowej w zakresie zwalczania prania pieniędzy jako przestępstwa transgranicznego. To oryginalny artykuł naukowy, którego celem jest ukazanie trudności, jakie w obliczu aktualnej sytuacji panującej na świecie rodzi współpraca z państwami trzecimi, tj. niebędącymi członkami Unii Europejskiej. Analizą objęto kilka obszarów tematycznych o znaczeniu istotnym dla poruszanych zagadnień (metoda formalno-dogmatyczna). Wskazano także na specyfikę regulacji obowiązujących w innych państwach, ważnych w szczególności w kontekście nowoczesnych technologii i zagrożeń procederem cyberprania pieniędzy (elementy metody prawno-porównawczej). W rezultacie wyprowadzono wnioski dotyczące problemów, jakie na arenie międzynarodowej, wykraczającej poza struktury unijne, rodzi walka z procederem „prania". W konkluzji wskazano na kierunki działań, jakich podjęcie byłoby pożądane w celu zapewnienia efektywnej współpracy międzynarodowej z krajami trzecimi w zakresie zwalczania prania pieniędzy.

Słowa kluczowe: pranie pieniędzy, kryptowaluty, kraje wysokiego ryzyka, raj finansowy, przemyt migrantów, wojna na Ukrainie

## COOPERATION WITH THIRD COUNTRIES IN COMBATING MONEY LAUNDERING IN THE FACE OF MODERN CHALLENGES

Abstract

The study is devoted to the issue of international cooperation in combating money laundering as a transnational crime. It is an original scientific article, the purpose of which is to show the difficulties that, in the face of the current situation in the world, are caused by cooperation

* dr hab., prof. UR, kierownik Zakładu Prawa Karnego w Instytucie Nauk Prawnych na Uniwersytecie Rzeszowskim (Polska), e-mail: agolonka@ur.edu.pl, ORCID: 0000-0002-0199-2203

Artykuł opublikowany w formule otwartego dostępu (open access) na licencji Uznanie autorstwa-Użycie niekomercyjne-Na tych samych warunkach 4.0 Międzynarodowe (CC BY-NC-SA 4.0) (https://creativecommons.org/licenses/by-nc-sa/4.0/).

with third countries, i.e. those that are not members of the European Union. The analysis covered several thematic areas that are of key importance in this regard (formal dogmatic method). The specificity of the regulations in force in other countries was also indicated, which are important, in particular, in the context of modern technologies and threats of cyber-laundering (elements of the legal and comparative method). As a result, conclusions were drawn regarding the problems that the fight against 'laundering' raises on the international arena, going beyond the structures of the EU. The conclusion indicates the directions of actions that would be desirable to undertake in order to ensure effective international cooperation with third countries in the field of combating money laundering.

Keywords: money laundering, cryptocurrencies, high-risk countries, financial haven, migrant smuggling, war in Ukraine

## WSTĘP

Przestępstwo prania pieniędzy to jedno z najpoważniejszych przestępstw gospodarczych zarówno pod względem skutków gospodarczych, jak i jego globalnej skali[1]. Zwalczanie tego procederu obejmuje nie tylko penalizowanie czynu, o którym mowa w art. 299 k.k.[2], ale również działania mające na celu przeciwdziałanie praniu pieniędzy[3]. W polskim prawie podstawowym aktem prawnym regulującym tę materię jest Ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (ustawa AML/CFT; Anti-Money Laundering/Counter Financing of Terrorism)[4]. Z uwagi na transgraniczny charakter, jaki zazwyczaj przybiera tytułowy proceder, immanentnie zresztą związany z jego złożoną naturą[5], zwalczanie prania pieniędzy na płaszczyźnie międzynarodowej nabiera szczególnej doniosłości. Poza działalnością prewencyjną, której trzon, w przypadku państw

[1] Szacuje się, że gospodarka światowa traci z tytułu prania pieniędzy corocznie ok. 2 do 5% światowego PKB, tj. ok. 1,87 bln euro, por. European Union Agency for Criminal Justice Cooperation – „Eurojust", *Money Laundering Cases Registered at Agency Doubled in Last 6 Years According to Eurojust's New Report* z 20.10.2022 r., https://www.eurojust.europa.eu/news/money-laundering-cases-registered-agency-doubled-last-6-years-according-eurojusts-new-report (dostęp: 7.03.2023).

[2] Ustawa z dnia 6.06.1997 r. Kodeks karny (Dz.U. z 2022 r., poz. 1138 ze zm.).

[3] Wypada zaznaczyć, że regulacje krajowe i międzynarodowe dotyczące przeciwdziałania praniu pieniędzy obejmują także przeciwdziałanie finansowaniu terroryzmu (AML/CFT). W tym opracowaniu zagadnienia odnoszące się do zwalczania finansowania terroryzmu zostaną pominięte.

[4] Ustawa z dnia 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2022 r., poz. 593 ze zm.).

[5] Najczęściej przyjmuje się, że pranie pieniędzy w „modelowym" ujęciu, zaproponowanym przez Grupę Specjalną ds. Przeciwdziałania Praniu Pieniędzy (The Financial Action Task Force, FATF), przebiega w trzech etapach. Są to: lokowanie (*placement*), maskowanie (*layering*) oraz legitymizacja (*integration*), por. np.: A. Golonka, *Prawnokarne zagadnienia przeciwdziałania wprowadzania do obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł*, Rzeszów 2008, s. 28–44 i powołana tam literatura, a także: https://www.iaml.com.pl/wiedza/etapy-prania-pieniedzy/ (dostęp: 15.02.2023). Niekiedy wskazuje się także na dodatkową fazę poprzedzającą wyżej wymienione, por. np.: P. Guberow, *Techniki prania brudnych pieniędzy*, w: *Pranie brudnych pieniędzy*, red. J. Grzywacz, Warszawa 2005, s. 24.

członkowskich Unii Europejskiej, wyznaczają niewątpliwie regulacje unijne AML[6], podejmowana jest również konkretna aktywność związana z działaniami strategicznymi oraz czynnościami operacyjnymi. Obecnie, co nie może być zaskoczeniem, zagrożenia w tej mierze wynikają przede wszystkim z sytuacji politycznej panującej na świecie, w tym z toczących się konfliktów zbrojnych, problemów ekonomicznych (na co niemały wpływ miała pandemia COVID-19), a także powszechnej cyfryzacji życia społecznego i gospodarczego. Kwestie te stanowiły asumpt do podjęcia rozważań nad implikacjami, jakie dla współpracy międzynarodowej w zakresie walki z procederem prania pieniędzy niosą wyzwania współczesnej rzeczywistości. Zagadnienie to nabiera szczególnej doniosłości w odniesieniu do relacji z tzw. krajami trzecimi[7] – określa się tym mianem zarówno państwa, które, z różnych względów, są uznawane za sprzyjające omawianemu procederowi (tzw. kraje wysokiego ryzyka[8]), jak i inne, które wprawdzie takiego statusu nie posiadają, ale pozostają poza strukturami unijnymi. W tym przypadku nie bez znaczenia pozostaje także kontekst, jakim jest aktualna sytuacja polityczna, ekonomiczna i społeczna, panująca na świecie. Równie istotne wydaje się uwzględnienie faktu, iż w dobie powszechnej cyfryzacji czyny sprawców przestępstw nierzadko sprowadzają się wyłącznie do ich aktywności w cyberprzestrzeni[9]. Odrębnym zagadnieniem staje się więc potrzeba zapewnienia bezpieczeństwa w przestrzeni cybernetycznej. Zwalczanie cyberprania pieniędzy (ang. *cyberlaundering*) stało się wręcz jednym z priorytetowych celów Unii Europejskiej i organizacji powołanych do zwalczania procederu „prania”[10].

---

[6] Na temat projektu unijnej nowelizacji i „zbioru AML” por. https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en (dostęp: 19.02.2023). Zagadnienie to jest na tyle obszerne, że jego wyczerpujące omówienie w niniejszym opracowaniu nie jest możliwe. Poświęcono mu miejsca na łamach osobnego opracowania pt. *Unijny projekt „pakietu AML” – reforma czy rewolucja w zakresie przeciwdziałania praniu pieniędzy*.

[7] Zgodnie z art. 2 pkt. 18 projektu rozporządzenia AML/CFT18: „państwo trzecie oznacza każdą jurysdykcję, niezależne państwo lub autonomiczne terytorium, które nie jest częścią Unii Europejskiej, ale które posiada własne przepisy w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu lub system ich egzekwowania”.

[8] Zgodnie z art. 9 dyrektywy 2015/849 pojęcie „państw trzecich wysokiego ryzyka” oznacza: „jurysdykcje państw trzecich, których krajowe systemy przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu wykazują strategiczne braki”. Z kolei w Ustawie z 1.03.2018 r. AML/CFT nakazuje objęcie tym terminem: każdego państwa identyfikowanego „na podstawie informacji pochodzących z wiarygodnych źródeł, w tym raportów z ewaluacji krajowych systemów przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu przeprowadzanych przez Grupę Specjalną do spraw Przeciwdziałania Praniu Pieniędzy (FATF) oraz organy lub organizacje z nią powiązane, jako nieposiadające skutecznego systemu przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu lub posiadające znaczące braki w systemie przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu”, uznając, iż jest to „w szczególności państwo trzecie zidentyfikowane przez Komisję Europejską w akcie delegowanym przyjętym na podstawie art. 9 dyrektywy 2015/849” (art. 2 ust. 2 pkt. 13 ustawy AML/CFT).

[9] Pojęcie cyberprzestrzeni oznacza: „przestrzeń aktywności ludzkiej z wykorzystaniem urządzeń elektronicznych do wytwarzania, przechowywania, przekazywania, przetwarzania i dostępu do informacji”, por. P. Dela, *Teoria walki w cyberprzestrzeni*, Warszawa 2020, s. 35.

[10] Por. także: M. Rojszczak, *Cyberbezpieczeństwo 2.0: w poszukiwaniu nowych ram ochrony cyberprzestrzeni*, w: *Cyberbezpieczeństwo*, red. C. Banasiński, J.M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, M. Rojszczak, K. Wałkowski, Warszawa 2020, s. 323–339; T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016,

Istotne trudności pojawiają się zarówno na płaszczyźnie stosowania prawa, jak i jego wykonania. Omówieniu tych kwestii zostanie poświęcone niniejsze opracowanie.

## PODSTAWY PRAWNE WSPÓŁPRACY MIĘDZYNARODOWEJ Z KRAJAMI TRZECIMI W ZAKRESIE ZWALCZANIA PRANIA PIENIĘDZY

Z uwagi na ponadnarodowy charakter, jaki w przeważającej większości przypadków przybiera pranie pieniędzy, jego efektywne zwalczanie jest możliwe jedynie przy sprawnej i dobrze skoordynowanej wzajemnej współpracy między państwami. Współpraca międzynarodowa w sprawach karnych (ang. *international cooperation in criminal matters*), niezależnie od kategorii czynów karalnych, do jakich się odnosi, ze swej natury obejmuje: „procedury wypracowane w kontaktach między państwami w związku ze sprawowaniem przez nie wymiaru sprawiedliwości w sprawach karnych”[11]. Jako taka opiera się więc na zasadach, które zapewniają poszanowanie tych procedur. Za najistotniejsze należy uznać zasady wzajemności oraz podwójnej karalności[12]. W piśmiennictwie wskazuje się także na obowiązywanie innych zasad, w tym stanowiących swoiste rozwinięcie tej pierwszej, tj. zasady wzajemności[13]. O trudnościach, jakie mogą pojawić się na gruncie poszanowania zasady wzajemności oraz podwójnej karalności napisano już niemało. Na łamach niejednego opracowania naukowego ukazywano je zarówno w szerszym aspekcie, tj. dotyczącym ogólnie ujętej współpracy międzynarodowej w sprawach karnych[14], jak i w węższym – obejmującym zwalczanie przestępczości gospodarczej[15]. Niektóre z opisanych już w literaturze

---

t. 8, z. 15, s. 20–22, 25. Na temat krajowej strategii „cyberbezpieczeństwa” por. *Strategia Cyberbezpieczeństwa RP na lata 2019–2024*, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 (dostęp: 3.01.2023); *Powstanie Centralne Biuro Zwalczania Cyberprzestępczości*, https://www.gov.pl/web/mswia/powstanie-centralne-biuro-zwalczania-cyberprzestepczosci oraz https://cbzc.policja.gov.pl/bzc/aktualnosci/92,Ruszyl-proces-doboru-do-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html (dostęp: 3.01.2023).

[11] Z. Barwina, *Zasada wzajemnego uznawania w sprawach karnych*, Warszawa 2012, s. 85.

[12] Ibidem, s. 43–84; M. Płachta, *Uznawanie i wykonywanie zagranicznych orzeczeń karnych. Zagadnienia podstawowe*, „Państwo i Prawo” 1985, nr 3, s. 88–89; J. Banach-Gutierrez, *Europejski wymiar sprawiedliwości w sprawach karnych. W kierunku ponadnarodowego systemu sui generis?*, Warszawa 2011, s. 156–208; G. Krysztofiuk, *Zasada wzajemnego uznawania orzeczeń w sprawach karnych w Traktacie Lizbońskim*, „Prokuratura i Prawo” 2011, nr 7, s. 11; A.J. Szwarc, J. Długosz, *Unijne instrumenty współdziałania państw w sprawach karnych*, „Edukacja Prawnicza” 2011, nr 3, s. 31–34; L. Brodowski, *Zasada podwójnej karalności czynu w kontekście ekstradycji*, „Studia Prawnicze KUL” 2015, nr 1, s. 31–58.

[13] Por. S. Steinborn, w: *Europejskie prawo karne*, red. A. Grzelak, M. Królikowski, A. Sakowicz, wyd. I, Warszawa 2012, s. 51–90.

[14] Por. np. G. Krysztofiuk, *Perspektywy współpracy sądowej w sprawach karnych w Unii Europejskiej*, „Prokuratura i Prawo” 2015, nr 7–8, s. 186–205; M.A. Liwo, *Współpraca transgraniczna Unii Europejskiej jako przejaw integracji narodów w zapewnieniu poczucia bezpieczeństwa*, „Przegląd Prawa Publicznego” 2013, nr 7–8, s. 89–92; P. Hofmański, *Przyszłość ścigania karnego w Europie*, „Europejski Przegląd Sądowy” 2006, nr 12, s. 4–11.

[15] P. Hofmański, *Przyszłość ścigania…*, op. cit., s. 5; A. Szumski, *Współpraca międzynarodowa w zwalczaniu przestępczości zorganizowanej na obszarach dawnych konfliktów etnicznych na przykładzie*

dylematów, gdy je odnosić do prania pieniędzy, nabierają nowego wymiaru. Tym bardziej że nierzadko w grę wchodzi „potrzeba wspólnego działania organów wymiaru sprawiedliwości trzech czy czterech państw, z których każde należy do innego kręgu i wplątane jest w sieci odmiennych zobowiązań i porozumień"[16].

Podwaliny prawnej współpracy międzynarodowej w zwalczaniu przestępczości zorganizowanej, w szczególności związanej z praniem pieniędzy, tworzą umowy bilateralne pomiędzy państwami oraz przede wszystkim międzynarodowe konwencje[17]. Do najistotniejszych, których stroną jest także Polska, należą niewątpliwie: Konwencja o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa, sporządzona w Strasburgu w dniu 8 listopada 1990 r.[18] oraz Konwencja Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzona w Warszawie dnia 16 maja 2005 r. (zwana Konwencją Warszawską)[19], zaś w szerszym aspekcie: Konwencja Narodów Zjednoczonych o zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi z 20 grudnia 1988 r.[20], Europejska Konwencja z dnia 20 kwietnia 1959 r. o pomocy prawnej w sprawach karnych[21] (zmieniona Drugim Protokołem Dodatkowym[22]), Konwencja o przekazywaniu osób skazanych, sporządzona w Strasburgu w dniu 21 marca 1983 r.[23] wraz z Protokołem Dodatkowym z dnia 18 grudnia 1997 r.[24] czy Układ z Schengen z dnia 19 czerwca 1990 r. wraz z Konwencją Wykonawczą (SIS II)[25], rozszerzającą zakres pomocy prawnej[26]. O obowiązywaniu tych regulacji wypada w tym miejscu jedynie wspomnieć, skoro meritum tego opracowania stanowi przede wszystkim ukazanie realnych trudności, jakie powstają we współpracy międzynarodowej z państwami trzecimi w kontekście aktualnych zagrożeń procederem „prania". Podobnie jak można przypomnieć o inicjatywach, jakie od wielu lat są podejmowane przez organizacje międzynarodowe powołane w celu jego zwalczania, a których członkiem

---

*misji EULEX Kosowo*, „Wschodnioznawstwo" 2016, nr 10, s. 93–100; I. Gawłowicz, M.A. Wasilewska, *Międzynarodowa współpraca w walce z przestępczością (międzynarodowe trybunały, Interpol)*, Szczecin 2004, s. 27–36.

16 P. Hofmański, *Przyszłość ścigania…*, op. cit., s. 5.

17 A. Wyrozumska, *Umowy międzynarodowe. Teoria i praktyka*, Warszawa 2007, s. 21–30, 57–68.

18 Dz.U. z 2003 r., nr 46, poz. 394, a także: A. Marek, *Komentarz do Konwencji w sprawie prania dochodów pochodzących z przestępstwa, ich ujawniania, zajmowania i konfiskaty*, w: *Standardy prawne Rady Europy. Teksty i komentarz. Tom III – Prawo karne*, red. E. Zielińska, Warszawa 1997, s. 561–568.

19 Dz.U. z 2008 r., nr 165, poz. 1028 wraz z Poprawką do Konwencji Rady Europy o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa oraz o finansowaniu terroryzmu, sporządzona w Warszawie 16.05.2005 r., przyjęta w Strasburgu 22.10.2014 r. (Dz.U. z 2018 r., poz. 1328).

20 Dz.U. z 1995 r., nr 15, poz. 69.

21 Dz.U. z 1999 r., nr 76, poz. 854.

22 Dz.U. z 2004 r., nr 139, poz. 1476.

23 Dz.U. z 1995 r., nr 51, poz. 279.

24 Dz.U. z 2000 r., nr 43, poz. 490.

25 Ustawa z 24.08.2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz.U. z 2021 r., poz. 1041 ze zm.) oraz zmiany obowiązujące od 1.01.2023 r. (Dz.U. z 2022 r., poz. 2642).

26 M. Aksamitowska-Kobos, *Wnioski sądów polskich o wykonanie orzeczeń w sprawach karnych dotyczących kar o charakterze pieniężnym kierowane za granicę*, „Iustitia" 2015, nr 1, s. 29.

jest także nasze państwo. Należą do nich w szczególności: Grupa Specjalna do spraw Przeciwdziałania Praniu Pieniędzy (FATF)[27], Grupa Egmont[28] czy Komitet Moneyval[29]. Ich roli w tym względzie nie sposób przecenić. Tym bardziej że opracowywane przez nie dokumenty zawierają m.in. analizy dotyczące tendencji w zakresie metod „prania", wskazują na obszary i instytucje najbardziej narażone na udział w procederze, a tym samym – wytyczają kierunki współpracy państw będących członkami tych organizacji. Działania tych instytucji mają istotne znaczenie z perspektywy dialogu międzynarodowego, którego rezultatem jest wypracowanie spójnych rozwiązań prawnych w dziedzinie prania pieniędzy. Nadal jednak pozostaje wiele obszarów, które z pespektywy omawianego procederu wymagają podjęcia szczególnych działań lub opracowania takich rozwiązań na płaszczyźnie międzynarodowej, które przyczynią się do poprawy w zakresie efektywności ścigania sprawców tego transgranicznego przestępstwa. Odnosi się to w szczególności do współpracy z państwami trzecimi. Wypada przy tym wskazać również na to, iż trudności we współpracy międzynarodowej z państwami trzecimi w zakresie zwalczania prania pieniędzy rodzi nie tyle samo to przestępstwo, które – jako *delictum iuris gentium* (przestępstwo prawa narodów), jest objęte zazwyczaj stosownymi porozumieniami bi- lub multilateralnymi, ile jego czyny bazowe.

## PROBLEM CZYNÓW BAZOWYCH W KONTEKŚCIE TRUDNOŚCI WE WSPÓŁPRACY Z PAŃSTWAMI TRZECIMI W ZWALCZANIU PRANIA PIENIĘDZY

Czyny bazowe prania pieniędzy (zwane także źródłowymi lub pierwotnymi[30]) to przestępstwa albo wykroczenia, z których pochodzą korzyści majątkowe, wprowadzane następnie do legalnego obrotu prawnego[31]. Przestępstwa bazowe sprawiają wiele trudności zarówno z dogmatycznego, jak i praktycznego punktu widzenia. Powodem tego jest nie tylko potrzeba wykazania związku takich czynów

---

[27] *The Financial Action Task Force* (FATF) została utworzona podczas szczytu państw G7, w Paryżu w 1989 r. Jej członkami jest obecnie 39 państw (w tym zawieszona w prawach członka od 24.02.2023 r. Federacja Rosyjska). Od 2007 r. FATF objęła procedurą weryfikacji AML/CFT 125 krajów. Więcej (w tym 40 Rekomendacji FATF) na stronie: https://www.fatf-gafi.org/en/home.html (dostęp: 22.02.2023).

[28] Informacje o organizacji, jej celach i bieżące raporty oraz strategia na lata 2022–2027 na oficjalnej stronie Grupy Egmont: https://egmontgroup.org/ (dostęp: 22.02.2023). Por. także: J. Grzywacz, *Pranie pieniędzy. Metody, raje podatkowe, zwalczanie*, Warszawa 2010, s. 160–161.

[29] Komitet Ekspertów ds. Oceny Systemów Zwalczania Procederu Prania Pieniędzy i Finansowania Terroryzmu (Moneyval) został utworzony w 1997 r. i jest stałym organem monitorującym Rady Europy, któremu powierzono zadanie oceny zgodności z podstawowymi międzynarodowymi standardami przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu i skuteczności ich wdrażania, a także przedstawiania władzom krajowym zaleceń dotyczących koniecznych usprawnień ich systemów. Więcej na: https://www.coe.int/en/web/moneyval (dostęp: 22.02.2023). Por. także: J.W. Wójcik, *Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Warszawa 2002, s. 133.

[30] J.W. Wójcik, *Przeciwdziałanie praniu pieniędzy*, Kraków 2004, s. 73–82.

[31] A. Golonka, *Prawnokarne zagadnienia…*, op. cit., s. 11–14.

z procederem „prania", ale niekiedy także te czyny *per se*. Odnosi się to m.in. do kwestii związanych z określeniem miejsca i sposobu ich popełnienia, ich statusu w porządku prawnym danego państwa, charakterystyki czynności sprawczej czy nawet okoliczności ich popełnienia. Stają się one szczególnie dyskusyjne w obliczu aktualnych zagrożeń i ich ukazaniu przez pryzmat wspomnianej już w tym opracowaniu zasady podwójnej karalności. Tym samym, chociaż samo to zagadnienie z całą pewnością nie stanowi żadnego *novum*, bowiem poświęcono mu pogłębione badania naukowe już niemal wiek temu[32], to jednak w kontekście czynów bazowych prania pieniędzy zasługuje na szczególną uwagę. Warto jednocześnie wskazać, jak trafnie podniesiono w piśmiennictwie, iż:

> Pojęcie podwójnej karalności należy rozumieć szeroko, co oznacza, że badając spełnienie warunku podwójnej karalności, należy nie tylko odwołać się do treści przepisu polskiej ustawy karnej, który mógłby odpowiadać przepisowi prawa państwa obcego, ale i do obowiązującej wykładni odnoszącej się do zakresu stosowania tego przepisu w systemie prawa polskiego. Oceniać należy bowiem całą sytuację faktyczną (…)[33].

W rezultacie wywiedziono także, iż:

> pojęciu podwójnej karalności należy nadawać różne znaczenie w zależności od tego, czy mówimy o spełnieniu tego warunku w sytuacji abstrakcyjnej – tzn. kiedy dane zachowanie jest zachowaniem zabronionym przez ustawę w obu państwach (tzw. podwójna karalność *in abstracto*) – czy też badamy możliwość postawienia sprawcy zarzutu dokonania danego przestępstwa w konkretnym stanie faktycznym, co może nastąpić dopiero po przeniesieniu konkretnego zachowania na grunt prawa polskiego (podwójna karalność *in concreto*)[34].

W odniesieniu do problemu karalności czynu w danym porządku prawnym, szczególnie problematyczne są przestępstwa skarbowe, w tym podatkowe. Wynika to z faktu, iż kryminalizacja takich czynów jest uzasadniona przede wszystkim potrzebą ochrony interesu finansowego danego państwa przed uszczupleniem należności publicznoprawnej lub narażeniem na nie (stosując nomenklaturę przyjętą w k.k.s.[35]). W prawie podatkowym mowa jest nawet o zjawisku międzynarodowej konkurencji podatkowej, które:

> Leży u źródeł zachowania niektórych państw, które przez modyfikację istniejącego prawodawstwa starają się zredukować obciążenia fiskalne nakładane w ich kraju na zagranicznych inwestorów, co ma spowodować szerszy napływ kapitału i zwiększyć tym samym stopę inwestycji[36].

---

[32] Por. np. S. Pszczółkowski, *Zagadnienie podwójnego opodatkowania w stosunkach międzynarodowych* (rozprawa doktorska przyjęta przez Radę Wydziału Prawa UW uchwałą z dnia 1.05.1925 r.), Warszawa 1928.

[33] Por. postanowienia SN z 22.11.2011 r., IV KK 267/11, OSNKW 2012, nr 3, poz. 24.

[34] Ibidem oraz: H. Kuczyńska, *Glosa do postanowienia Sądu Najwyższego z dnia 22 listopada 2011 r., sygn. IV KK 267/11*, „Prokuratura i Prawo" 2013, nr 3, s. 171, a także: L. Gardocki, *Podwójna przestępność czynu w prawie ekstradycyjnym*, w: *Problemy nauk penalnych. Prace ofiarowane Pani Profesor Oktawii Górniok*, Katowice 1996, s. 70–72.

[35] Art. 53 §§ 26 i 26a k.k.s., Dz.U. z 2022 r., poz. 859 ze zm.

[36] J. Grzywacz, *Pranie pieniędzy. Metody, raje…*, op. cit., s. 57.

Zagadnienia dotyczące współpracy międzynarodowej w zakresie prawa podatkowego, w tym wymiany informacji między państwami[37], poparte stosownymi regulacjami[38], czy aspekty legalności unikania opodatkowania[39], były już przedmiotem odrębnych opracowań. W niniejszym, odnoszącym się wszak do prania pieniędzy, wypada zwrócić uwagę na szczególnie problematyczną w tym względzie współpracę międzynarodową z państwami uznawanymi za tzw. „raje podatkowe". Za raj finansowy, zwany także oazą lub azylem podatkowym lub jurysdykcją *offshore*[40], uznaje się: „obszar, w którym istnieje system prawny umożliwiający podmiotom zagranicznym redukcję obciążeń podatkowych w ich macierzystych krajach"[41]. Współpraca z takimi państwami rodzi trudności wynikające m.in. z braku transparentności podatkowej względem innych państw i odpowiednich instytucji państwowych, braku chęci do jej podjęcia z powoływaniem się na krajowe, restrykcyjne unormowania dotyczące ochrony tajemnicy (np. Honkong, Kajmany), stosowania niskich stawek podatkowych, liberalnych przepisów określających zasady prowadzenia działalności gospodarczej etc.[42] Państwa – raje finansowe, chociaż najczęściej są stronami konwencji międzynarodowych – w szczególności tych wymienionych powyżej, to jednak z racji zgłoszonych do nich zastrzeżeń[43], niejednokrotnie czynią współpracę podejmowaną na ich podstawie praktycznie niemożliwą. Warto także przypomnieć, że państwa, które nie uchodzą za oazy podatkowe ani w świetle wykazów FATF ani dokumentów wydanych przez inne instytucje krajowe[44]

---

[37] B. Kuźniacki, *Wymiana informacji podatkowych z innymi państwami. Nowa era stosowania prawa podatkowego w wymiarze międzynarodowym. Wymiana informacji o rachunkach finansowych, interpretacjach podatkowych oraz informacji o jednostkach z grupy* (*cz. 2*), „Przegląd Podatkowy" 2017, nr 6, s. 17–30.

[38] Ustawa z 9.03.2017 r. o wymianie informacji podatkowych z innymi państwami (Dz.U. z 2023 r., poz. 241).

[39] J. Jankowski, *Klauzula przeciwko unikaniu opodatkowania (GAAR). Przepisy materialnoprawne*, Warszawa 2022, s. 21–22; o „międzynarodowym planowaniu podatkowym" (tj. stosowaniu legalnych mechanizmów celem ograniczenia lub wyeliminowania opodatkowania dochodów lub majątku, akumulacji dochodów przez odpowiednie wykorzystanie rajów podatkowych) zob. J. Grzywacz, *Pranie pieniędzy. Metody, raje…*, op. cit., s. 57.

[40] J. Grzywacz, *Pranie pieniędzy. Metody, raje podatkowe…*, op. cit., s. 51.

[41] Ibidem, s. 52.

[42] J.F. Mika, M. Mika, *Istota rajów podatkowych*, w: *Raje podatkowe. Procedura należytej staranności, obowiązki w cenach transferowych*, red. J.F. Mika, Warszawa 2023, s. 3, 13–15.

[43] Np. do Konwencji strasburskiej z 1990 r. o praniu, ujawnianiu, zajmowaniu i konfiskacie dochodów pochodzących z przestępstwa w zakresie odmowy wykonywania wniosków w razie braku podwójnej karalności w odniesieniu do przestępstw źródłowych dla prania pieniędzy (Andora, Antyle Niderlandzkie, Aruba, Monako); ograniczenie wykorzystania informacji tylko do postępowania, w ramach którego wystąpiono z wnioskiem (Andora, Antyle Niderlandzkie, Aruba, Lichtenstein, Monako); wykonywania wniosku tylko zgodnie z prawem krajowym danego państwa – „z poszanowaniem zasad konstytucyjnych" oraz „podstawowych koncepcji prawnych" (Andora, Antyle Niderlandzkie, Aruba, Lichtenstein, Monako, Wyspa Man, Guernsey); odmowy wykonania wniosku w przypadku możliwości zakwalifikowania przestępstwa będącego podstawą wniosku, jako czynu o charakterze podatkowym lub celnym (Antyle Niderlandzkie, Aruba); C. Michalczuk, *Współpraca prawna w sprawach karnych z „rajami podatkowymi"*, „Prokuratura i Prawo" 2010, nr 9, s. 138–139.

[44] Obwieszczenie Ministra Finansów w sprawie ogłoszenia listy krajów i terytoriów wskazanych w unijnym wykazie jurysdykcji niechętnych współpracy do celów podatkowych przyjmowanym przez Radę Unii Europejskiej, które nie zostały ujęte w wykazie krajów i terytoriów

i zagraniczne[45], wprowadzają także restrykcyjne regulacje np. dotyczące ochrony tajemnicy bankowej czy zasad przekazywania pewnych informacji (np. Stany Zjednoczone, Szwajcaria). Tym samym utrudniają one współpracę z nimi innych państw w sprawach dotyczących podejrzenia prania pieniędzy.

## CYBERLAUNDERING JAKO WYZWANIE DLA WSPÓŁPRACY MIĘDZYNARODOWEJ W WALCE Z TYM ZJAWISKIEM

Analizując aspekty związane z aktualnymi zagrożeniami i rozpatrując je w kontekście podwójnej karalności, nie sposób byłoby nie wspomnieć o cyberlaunderingu, a także o innych przestępstwach popełnionych w cyberprzestrzeni, stanowiących zarazem czyny bazowe „prania". Przybierają one postać *cybercrimes* lub *cyber-enabled crimes*[46], a więc cyberprzestępstw albo przestępstw popełnionych przy wykorzystaniu elektronicznych dróg komunikacji (na czele z przekrętem nigeryjskim[47]). W praktyce mogą przy tym obejmować wiele bardzo zróżnicowanych pod względem charakteru i przebiegu czynów. Najczęściej popełnianymi cyberprzestępstwami, z których pochodzą korzyści wprowadzane następnie do legalnego obrotu, pozostają jednak różne formy i metody oszustw internetowych (*fraud*, *scamm*, *phishing*, *spoofing*, *pharming* etc.)[48]. Znajduje to potwierdzenie w raportach instytucji powołanych do zwalczania prania pieniędzy – zarówno krajowych[49], jak i zagranicznych[50]. Nie powinno

---

stosujących szkodliwą konkurencję podatkową wydawanym na podstawie przepisów o podatku dochodowym od osób fizycznych oraz przepisów o podatku dochodowym od osób prawnych, oraz dnia przyjęcia tego wykazu przez Radę Unii Europejskiej z 10.03.2022 r., „Monitor Prawniczy" poz. 341, a także: J.F. Mika, M. Mika, w: *Raje podatkowe…*, op. cit., s. 13–14.

[45] Por. dokumenty z posiedzenia Rady do Spraw Gospodarczych i Finansowych w sprawie unijnego wykazu jurysdykcji niechętnych współpracy z dnia 14.02.2023, na: https://www.consilium.europa.eu/pl/press/press-releases/2023/02/14/taxation-british-virgin-islands-costa-rica-marshall-islands-and-russia-added-to-eu-list-of-non-cooperative-jurisdictions-for-tax-purposes/ (dostęp: 14.03.2023).

[46] Na temat wąskiego oraz szerokiego ujęcia cyberprzestępstwa por. *Online African Organized Crime from Surface to Darkweb*, Raport analityczny UE i INTERPOL-u, 2020, s. 12.

[47] Przekręt nigeryjski (zwany także afrykańskim szwindlem, *Nigerian scam* lub „419 scam") to: „rodzaj oszustwa, polegającego na namówieniu ofiary na transfer pieniędzy do jednego z krajów afrykańskich (początkowo Nigerii) w celu uzyskania dużej korzyści" – por. R. Balkowski, *Bezpieczeństwo systemów teleinformatycznych – zmiany, trendy i zasady*, Warszawa 2018, s. 9, a także przykład procederu „prania" z wykorzystaniem „419 scam" – E.I. Hartikainen, *The Nigerian Scam: Easy Money on the Internet, But For Whom?*, Michigan 2006, s. 1–2, 4–5.

[48] Por. B/A, *Scams & Swindles: Phishing, Spoofing, ID Theft, Nigerian Advance Schemes, Investment Frauds, False Sweethearts: How to Recognize and Avoid Financial Rip-offs in the Internet Age*, wyd. I, Los Angeles 2006, s. 43–244, a także: J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 126–131.

[49] *Sprawozdanie Generalnego Inspektora Informacji Finansowej z realizacji ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w 2021 roku*, Warszawa, marzec 2022. Dokument do pobrania na stronie: https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej (dostęp: 26.08.2023).

[50] Por. IEWG, *FIU-FinTech Cooperation and Associated Cybercrime Typologies and Risks*, Ottawa, July 2022, s. 35–37. Dokument do pobrania na stronie Egmont: https://egmontgroup.org/ (dostęp: 3.03.2023); European Union Agency for Criminal Justice Cooperation-Eurojust, *Money*

budzić wątpliwości, że do znacznego wzrostu liczby *sensu largo* ujętych[51] oszustw „w sieci"[52] przyczyniła się globalna sytuacja związana z pandemią COVID-19[53]. Wystarczy wskazać, że Interpol już w pierwszych miesiącach 2020 r. skierował do Policji wszystkich (ówczesnych 194) krajów członkowskich alert (*Urgent Safety Alert*), zawierający ostrzeżenie na temat podwyższonego ryzyka ataków *ransomware*[54], nowych technik i sposobów działania cyberprzestępców[55]. Pod auspicjami Interpolu została także przeprowadzona w 2020 r. „operacja Pangea XIII", w którą zaangażowały się służby państwowe 90 krajów[56]. Była ona wymierzona w zorganizowane grupy przestępcze, prowadzące nielegalną działalność w zakresie obrotu „w sieci" medykamentami oraz parafarmaceutykami. W jej wyniku aresztowano 121 osób na całym świecie i podjęto czynności związane z zabezpieczeniem mienia o łącznej wartości ponad 14 mln dolarów[57].

Korzyści poddawane „praniu" pochodzą również z cyberprzestępstw o charakterze seksualnym (*sextortion*)[58], różnych form handlu ludźmi w Internecie[59], handlu narkotykami i innymi substancjami odurzającymi w Darknecie[60], handlu narządami etc.[61] To jedynie wąski „wycinek" spośród wielu przestępstw, do jakich dochodzi w cyberprzestrzeni – począwszy od tych popełnianych przy wykorzystaniu usług finansowych świadczonych drogą internetową i mobilną (w tym obejmujących bankowość internetową i mobilną) lub za pośrednictwem platform finansowania społecznościowego, po coraz częściej popełniane przestępstwa przy wykorzystaniu

---

*Laundering Cases Registered at Agency Doubled in Last 6 Years According to Eurojust's New Report* z 20.10.2022 r., s. 6, 39.

[51] Na temat różnic między *fraud* a *scam* por. A. Golonka, *Scamming*, w: *Przestępczość zorganizowana. Aspekty prawne kryminalno-kryminalistyczne*, red. P. Łabuz, I. Malinowska, M. Michalski, Warszawa 2022, s. 290–303.

[52] C. Weerth, *INTERPOL on COVID-19: COVID-19 Crime and Fraud Alert*, „Technical Raport" 2020, April, s. 1–4. DOI:10.13140/RG.2.2.33650.25282

[53] *Jak przestępcy wykorzystują pandemię*, (KWP w Białymstoku) „Policja 997" 2020, nr 182, s. 47–48.

[54] Aktualny stan zagrożenia atakami *ransomware* por. *2022 SonicWall Cyber Threat Raport*, wprowadz. B. Conner, s. 12–20. Do pobrania na: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf (dostęp: 26.10.2023).

[55] Terminologia dotycząca sprawców cyberprzestępstw (hackerów i crakerów) por. M. Zaród, *Hakerzy i kolektywy hakerskie w Polsce. Od operacjonalizacji do laboratoriów i stref wymiany*, „Przegląd Socjologiczny" 2017, t. 1, z. 224, s. 227–228, a także: idem, *Aktorzy-sieci w kolektywach hakerskich*, s. 50, 54 (rozprawa doktorska, Instytut Socjologii UW, Warszawa 2018). Do pobrania w repozytorium na: https://depotuw.ceon.pl/handle/item/2909 (dostęp: 26.02.2023).

[56] C. Weerth, *INTERPOL on COVID-19: Urgent Safety Alert – Results of the 2020 Fake Medicine and Medicine Products Operation PANGEA XIII*, „Technical Report" 2020, March, s. 1–4. DOI:10.13140/RG.2.2.13950.95040.

[57] Ibidem, s. 1–2.

[58] Por. *Online African Organized Crime…* (Raport 2020), op. cit., s. 20–32.

[59] Ibidem.

[60] Na temat handlu narkotykami w Darknecie: G. Ocieczek, P. Opitek, *Praktyczne aspekty zwalczania przestępczości narkotykowej dokonywanej w „świecie realnym" i cyberprzestrzeni*, „Prokuratura i Prawo" 2022, nr 7–8, s. 243–251. Por. także: *Scams & Swindles…*, op. cit., s. 133–148.

[61] Por. R. Kumar, *Kidney Transplants and Scams: India's Troublesome Legacy*, New Delhi 2020, s. 39–69, 131–164.

aktywów wirtualnych (*virtual asset*, VA)[62]. W piśmiennictwie wskazuje się nawet, że wykorzystywanie walut wirtualnych do wspierania nielegalnej aktywności, w tym do celu prania pieniędzy jest aktualnie jednym z najbardziej niebezpiecznych zjawisk zarówno dla systemów finansowych poszczególnych państw[63], jak i dla całej światowej społeczności[64].

## KRYPTOAKTYWA JAKO ŹRÓDŁO SZCZEGÓLNEGO ZAGROŻENIA PRANIEM PIENIĘDZY W RELACJACH Z PAŃSTWAMI TRZECIMI

Działania w zakresie walki z praniem pieniędzy, prowadzone przez organizacje i instytucje międzynarodowe, sprowadzają się więc przede wszystkim do opracowania mechanizmów pozwalających na ochronę systemów finansowych przed tym procederem. Z oczywistych względów pożądaną (i oczekiwaną) jest współpraca opierająca się na standardach wypracowanych na forum międzynarodowym. Rolę światowego „gwaranta" w dziedzinie zapobiegania i zwalczania prania pieniędzy pełni niewątpliwie Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy (FATF). W dniu 28 października 2021 r. FATF zaprezentowała zaktualizowany przewodnik podejścia opartego na ryzyku (*Risk-Based Approach*)[65]. Organizacja ta zwraca w nim uwagę m.in. na konieczność stosowania przez operatorów usług aktywów wirtualnych takich samych środków bezpieczeństwa finansowego, jakie dotyczą innych podmiotów zobowiązanych. Wobec tego VASP-y powinna obowiązywać w szczególności należyta staranność wobec klienta (CDD), prowadzenie dokumentacji, monitorowanie transakcji i zgłaszanie tych podejrzanych (STR). „Pod lupą" znaleźli się więc m.in.: kryptogiełdy, operatorzy kriptomatów, fundusze *hedgingowe* obsługujące kryptowaluty, administratorzy kryptoportfeli czy administratorzy stablecoinów[66]. Uaktualniony dokument: „40 Rekomendacji" FATF przewiduje obecnie zalecenia dotyczące licencjonowania i rejestracji VASP-ów, a także dodatkowe rekomendacje dotyczące wdrażania *Travel Rule*[67]. W ocenie FATF realizacja tych wytycznych warunkuje sprawną i efektywną współpracę w zakresie zwalczania tej formy *cyberlaunderingu*, zapewniając przy tym przejrzystość transakcji przeprowadzanych przy użyciu aktywów wirtualnych.

---

62 Na temat terminologii por. A. Behan, *Waluty wirtualne…*, op. cit., s. 237–242. K. Krasuski, O. Kharif, (Bloomberg News): *Crypto Capital Official Nabbed in Polish Money Laundering Probe*, https://www.bnnbloomberg.ca/crypto-capital-official-nabbed-in-polish-money-laundering-probe-1.1337624 (dostęp: 10.01.2023).

63 Postępowanie z udziałem polskiej Prokuratury por. np.: K. Krasuski, O. Kharif (Bloomberg News): *Crypto Capital Official Nabbed in Polish Money…*, op. cit.

64 P. Opitek, *Przeciwdziałanie praniu pieniędzy…*, op. cit., s. 54.

65 FATF, *Virtual Assets*, https://www.fatf-gafi.org/en/topics/virtual-assets.html oraz FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (dostęp: 26.02.2023).

66 IEWG, *FIU-FinTech…*, op. cit., s. 4.

67 Rekomendacja 16 FATF nakładająca obowiązek identyfikacji klienta i beneficjenta (VASP) oraz gromadzenia i przechowywania transakcji finansowych z wykorzystaniem VA.

Z perspektywy, o której mowa w tym opracowaniu, podstawowym problemem staje się podwójna karalność przestępstw popełnionych z wykorzystaniem aktywów wirtualnych. Wystarczy wskazać na daleko idące różnice w unormowaniach. Przykładowo w państwach takich jak Algieria, Boliwia, Maroko, Nepal, Pakistan czy Wietnam zakazana jest wszelka działalność związana z kryptowalutami[68]. Z kolei w innych, jak w Katarze i Bahrajnie, jest ona dopuszczalna dla obywateli tych państw, ale pod warunkiem, że sama działalność jest wykonywana poza granicami tych krajów. Są i takie jurysdykcje (m.in. Bangladesz, Iran, Tajlandia, Kolumbia, Chiny – od 2021 r.), w których dopuszczalne są tylko transakcje prywatne[69], albo obowiązuje tylko częściowy zakaz obrotu kryptowalutami (np. Iran od 2022 r. dopuszcza transakcje kryptowalutami w imporcie[70]). Można wreszcie wskazać i na takie rozwiązania prawne, jak obowiązujące od 2017 r. w Chińskiej Republice Ludowej, które ustanawiają zakaz *Initial Coin Offering* (ICO), czyli pozyskiwania kryptowalut lub tokenów cyfrowych drogą *crowdfundingu* (finasowania społecznościowego) – na wzór pierwszej publicznej oferty (zazwyczaj nowych) tokenów[71]. Niedawno, we wrześniu 2021 r., chiński rząd uznał także wszystkie prywatne transakcje związane z kryptowalutami za nielegalne, powołując się na obawy dotyczące inwestycji spekulacyjnych, ekstremalnej zmienności cen, oszustw związanych z hazardem i prania pieniędzy[72].

Dostrzegając zagrożenia płynące z wykorzystania kryptowalut do celu prania pieniędzy, należy także pamiętać o tych czynach bazowych, które stanowią (teoretycznie) „tradycyjne" przestępstwa. Mowa np. o włamaniach, wymuszeniach okupu, kradzieży, przywłaszczeniu etc., jednak popełnionych przy wykorzystaniu nowoczesnych technologii *blockchain*[73] (względnie np. metody *hash tree*, wykorzystywanej przez *Ripple* w transakcjach kryptowalutą XRPs[74]). Przykładami takich przestępstw są: włamania do elektronicznych portfeli, wymuszenia okupu

---

[68] Za: J. Riley, *The Current Status of Cryptocurrency Regulation in China and Its Effect around the World*, „China and WTO Review" 2021, vol. 7 (1), s. 139, http://dx.doi.org/10.14330/cwr.2021.7.1.06 (dostęp: 26.10.2023).

[69] J. Riley, *The Current Status of Cryptocurrency…*, op. cit., s. 139.

[70] Zob. www.iranintl.com/en/202208293261 (dostęp: 26.10.2023). Na temat trudności z transakcjach bitcoinem i irańskiej walucie cyfrowej PayMon**,** zabezpieczonej złotem: https://bitcoinpl.org/iranskia-waluta-cyfrowa-paymon (dostęp: 27.02.2023). Na temat e-Gold i zabezpieczenia kryptowaluty złotem por. A. Behan, *Waluty wirtualne…*, op. cit., s. 40–46.

[71] Ibidem, s. 139–146, a także: F. Allen, X. Gu, J. Jagtiani, *Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China*, „Working Papers – Federal Reserve Bank of Philadelphia" 2022, vol. 22 (4), s. 3, https://doi.org/10.21799/frbp.wp.2022.12 (dostęp: 26.10.2023).

[72] F. Allen, X. Gu, J. Jagtiani, *Fintech, Cryptocurrencies, and CBDC…*, op. cit., s. 3.

[73] *Blockchain* (technologia *blockchain*) to „łańcuch bloków", które służą do przechowywania i przesyłania informacji o transakcjach zawartych w Internecie. Jej praktyczne znaczenie polega na możliwości przekazania przez jeden podmiot drugiemu „unikatowego fragmentu internetowych praw własności w sposób bezpieczny, jawny i na takich warunkach, że nikt nie może zakwestionować legalności takiej transakcji", por. J. Zych, *Teleinformatyka dla bezpieczeństwa*, wyd. II, Poznań 2019, s. 133–134.

[74] Por. M. Kowalczyk, *Ripple – czym jest i czy warto zainwestować?* (cykl: kryplowaluty z 11.10.2021 r.). Dostępny na: https://www.najlepszekonto.pl/ripple-czym-jest-czy-inwestowac (dostęp: 25.02.2023), a także o walucie cyfrowej XRP: O. McDonalds, *Cryptocurrencies: Money, Trust and Regulation*, Newcastle 2021, s. 29–32.

w kryptowalutach, *cryptojacking*[75] czy przywłaszczenie (nierzadko nielegalnie uzyskanych) bitcoinów[76]. Co interesujące, sam proceder „prania", nawet popełniany przy wykorzystaniu waluty wirtualnej, nierzadko opiera się na metodach „prania" znanych od lat, czyli na *smurfingu* i *structuringu*[77]. Tym samym transakcje bazują np. na rachunkach zakładanych przez „słupy", które są przez nie wymieniane na kryptowaluty, a następnie transferowane do portfeli kryptowalutowych prowadzonych przez lokalnych operatorów usług aktywów wirtualnych. Przykładem jest proceder na wielką skalę, jaki miał miejsce w RPA, wykryty na podstawie raportu transakcji podejrzanych złożonego przez lokalny VASP[78]. Polegał on na zakupie dużych sum wirtualnych aktywów przez różne osoby i ich natychmiastowym transferze do zagranicznych VASP-ów. W wielu przypadkach różne osoby miały ten sam adres zamieszkania, a większość adresów tych wartości była dostępna z tego samego adresu IP. Nasunęło to podejrzenie wykorzystania ich jako „słupów" do „wyprania brudnych pieniędzy". Aby utrudnić wykrycie pochodzenia nielegalnych wartości majątkowych, na pierwszym etapie przeprowadzano transakcje gotówkowe, polegające na zdeponowaniu środków na różnych rachunkach w różnych instytucjach finansowych. Następnie były one przekazywane drogą płatności elektronicznych na inne rachunki po to, by finalnie nabyć za nie kryptowalutę (bitcoiny) w lokalnych VASP-ach. W proceder ten było zaangażowanych ponad 150 osób, odpowiedzialnych za przekazanie łącznie około 108 352 900 USD (11 960 bitcoinów)[79]. Innym przykładem „prania" za pomocą VASP-ów było wykorzystanie kryptogiełdy w Korei Południowej, za pośrednictwem której „wyprano" około 400 milionów wonów[80] (ponad 300 000 euro), pochodzących z *phishingu*. W tym przypadku pieniądze (z *phisingu*), zatem waluta fiducjarna, były wymieniane na trzy różne rodzaje kryptowalut, w ramach wielu transakcji, po to, aby po transferze trafić do jednego portfela zagranicznego VASP[81]. Szczególne niebezpieczeństwo dostrzega się w udziale

---

[75] Według definicji Urzędu Komisji Nadzoru Finansowego *cryptojacking* to: „rodzaj cyberprzestępczości polegający na zainfekowaniu i wykorzystaniu bez wiedzy i zgody użytkownika mocy obliczeniowej urządzenia zaopatrzonego w procesor (…) do wydobywania kryptowalut": https://cebrf.knf.gov.pl/encyklopedia/hasla/385-definicje/797-cryptojacking (dostęp: 26.10.2023). Por. także: K. Kropopek, *„Cryptojacking" wzrósł do rekordowego poziomu, pomimo załamania na rynku*, https://comparic.pl/cryptojacking-wzrosl-do-rekordowego-poziomu-pomimo-zalamania-na-rynku/ (dostęp: 26.02.2023), oraz: *2022 SonicWall Cyber Threat…*, op. cit., s. 31–33.

[76] G. Ocieczek, P. Opitek, *Praktyczne aspekty…*, op. cit., s. 247–248.

[77] *Smurfing* polega na przeprowadzaniu wielu operacji finansowych (m.in. celem rozdrobnienia wartości aktywów) przez wiele podstawianych w tym celu osób (tzw. słupy, muły), natomiast *structuring*, uznawany za odmianę tego pierwszego, sprowadza się do wielu wpłat powtarzalnych na dany rachunek (także „cząstkowy") – por. A. Golonka, *Prawnokarne zagadnienia przeciwdziałania…*, op. cit., s. 31–33, a także: W. Jasiński, *Pranie brudnych pieniędzy*, Warszawa 1998, s. 69–70; J.W. Wójcik, *Pranie pieniędzy. Kryminologiczna i kryminalistyczna…*, op. cit., s. 108–111 (określając je mianem technik rozdrabniania wpłat).

[78] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, s. 6, https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html (dostęp: 18.02.2023).

[79] Ibidem.

[80] Won południowokoreański (KRW) jest oficjalną walutą Korei Południowej.

[81] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, s. 7, https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html (dostęp: 18.02.2023).

kryptogiełd w krajach takich jak Chiny (pomimo obowiązujących w tym kraju stosunkowo restrykcyjnych regulacji dotyczących obrotu kryptowalutami[82]) czy Korea Północna (umieszczona zresztą przez FATF na „czarnej liście"), gdzie w 2022 roku doszło do kradzieży kryptowalut o wartości ok. 1,7 mld dolarów – według danych szacunkowych[83]. Precyzyjniej, jak twierdzą eksperci, Korea Północna „zwraca się ku kradzieży kryptowalut, aby sfinansować swój arsenał nuklearny"[84]. Kryptowaluty są „prane" za pomocą tzw. mikserów (*mixers*), które bazując na metodzie znanej jako *blending*, mieszają kryptowaluty od różnych użytkowników, aby w ten sposób zgubić ślad pochodzenia tych aktywów. Istnieją także doniesienia o korzystaniu w tym celu z usług brokerów w Chinach i niezamiennych tokenów (NFT)[85].

Wybór opisanych tu przykładów prania pieniędzy z wykorzystaniem kryptowalut i udziału w nich VASP-ów zlokalizowanych w Chinach i Korei Północnej nie był przypadkowy. Państwa te stosunkowo często wskazywane są bowiem jako źródło potencjalnego zagrożenia ich udziałem w „praniu" waluty wirtualnej. W odniesieniu do Chin i Hongkongu mówi się zresztą o tym wprost[86]. Wskazuje się na to, że: „południowoamerykańskie kartele zajmujące się produkcją i handlem narkotykami korzystają z walut wirtualnych do wyprania pieniędzy w Chinach i Hongkongu. Bitcoin (…) pretenduje do miana międzynarodowego środka rozliczeń narkobiznesu"[87]. Zagrożenie dostrzega także amerykański Financial Crimes Enforcement Network (FinCEN)[88], który uznał zarejestrowaną w Hongkongu kryptogiełdę „Bitzlato" (*Bitzlato Limited*) za „główny problem związany z praniem brudnych pieniędzy"[89]. „Bitzlato" oferowała wymianę kryptowalut i szczególnie „podatnej" na pranie pieniędzy usługi *Peer-to-Peer* (P2P). Celem było zaś finansowanie nielegalnych operacji rosyjskich. Odbywało się to również dzięki współpracy m.in. z Hydra Market – rosyjskojęzycznym czarnym rynkiem (tj. działającym w Darknecie) i objętym sankcjami nałożonymi na Rosję po jej inwazji na Ukrainę. Darknet Hydra został

---

[82] W Chinach zakazem jest objęty *Initial Coin Offering* (ICO). O tym oraz zmianach w chińskim prawie regulującym obrót wirtualnymi aktywami por. F. Allen, X. Gu, J. Jagtiani, *Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China*, „Working Paper – Federal Reserve Bank of Philadelphia" 2022, vol. 22 (4), s. 3.

[83] Por. Kelly Ng (BBC News), *Crypto theft: North Korea-linked hackers stole $1.7b in 2022*, z 2.02.2023 r., https://www.bbc.com/news/world-asia-64494094 (dostęp: 25.02.2023).

[84] Ibidem, a także: FinCEN, https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack (dostęp: 25.02.2023).

[85] Kelly Ng (BBC News), *Crypto theft…*, op. cit.

[86] P. Opitek, *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 54–55.

[87] Ibidem, s. 54.

[88] https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering (dostęp: 27.02.2023).

[89] Założycielem „Bizlato" jest Rosjanin Anatoly Legkodymov (aresztowany przez amerykański Departament Sprawiedliwości w dniu 17.01.2023 r.), por. M. Garcia, L. Sinaina, *Bitzlato Founder Charged With Facilitating Money Laundering of More than $700 Million in Dark Web Funds*, z 3.02.2023, https://www.whitecase.com/insight-alert/bitzlato-founder-charged-facilitating-money-laundering-more-700-million-dark-web (dostęp: 25.02.2023).

zamknięty w dniu 4 kwietnia 2022 r.[90] Sankcjami objęto także Garantex[91], uznawany za najważniejszą platformę, służącą cyberprzestępcom do prania pieniędzy[92].

Od dnia 1 lutego 2023 r. w Stanach Zjednoczonych obowiązuje również regulacja ustanawiająca oficjalny zakaz transferu „Bitzlato"[93]. Faktem pozostaje jednak to, że sankcje i inne restrykcje nałożone na handel z Rosją[94] nie tylko nie wyeliminowały zagrożeń związanych z jej możliwym udziałem w procederze prania, ile ujawniły nowe przypadki prania „rosyjskich pieniędzy". Wskazuje się, że stan Dakota Południowa (USA) aspiruje nawet do miana prawdziwego raju podatkowego światowej klasy, a to za sprawą obowiązujących w tam przepisów regulujących zasady zakładania i prowadzenia „trustów"[95]. W istocie zaś firmy zakładane pod postacią funduszy powierniczych umożliwiają lokowanie w nich anonimowo środków finansowych, także rosyjskim oligarchom. Twierdzi się nawet, iż: „w funduszach powierniczych w Południowej Dakocie znajduje się ponad 350 mld dolarów, a stanowa legislatura (…) została tak całkowicie opanowana przez branżę trustów, że nie ma szans na zmianę przepisów"[96]. Do tego dochodzi swoisty „podwójny standard" obowiązujący w Stanach Zjednoczonych, jak określa się sytuację, w której: „rząd Stanów Zjednoczonych żąda informacji [dotyczących transakcji finansowych – przyp. aut.] od innych krajów, sam zaś odmawia dzielenia się informacjami o udziałach obcokrajowców w swoich bankach"[97]. Nie ułatwia to współpracy z tym państwem w zakresie przeciwdziałania praniu pieniędzy. Sygnalizuje się także istnienie luk w obowiązujących przepisach amerykańskich regulujących zasady raportowania transakcji podejrzanych. W rezultacie dochodzi do sytuacji, w której: „Gdy bank złoży raport o podejrzanej działalności, może swobodnie dalej prowadzić interesy z podejrzanym klientem, bo większość raportów, które nie są publicznie dostępne, pokrywa się cyfrowym odpowiednikiem kurzu"[98].

---

[90] Dr Hack, *Największy na świecie rynek Darknet zamknięty*, z 6.04.2022 r., https://satkurier.pl/news/216131/najwiekszy-na-swiecie-rynek-darknet-zamkniety.html (dostęp: 25.02.2023).

[91] U.S. Department of the Treasury, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, https://home.treasury.gov/news/press-releases/jy0701 (dostęp: 12.03.2023).

[92] *Rosyjscy cyberprzestępcy szukają nowych sposobów prania pieniędzy. Wszystko przez wojnę*, https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjscy-cyberprzestepcy-szukaja-nowych-sposobow-prania-pieniedzy-wszystko-przez-wojne (dostęp: 12.03.2023).

[93] Sekcja 9714(a) ustawy o przeciwdziałaniu praniu pieniędzy w Rosji (Combating Russian Money Laundering Act; Public Law 116–283), zmienionej S. 6106(b) National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81).

[94] U.S. Department of the Treasury, *Ukraine-/Russia-related Sanctions*, https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions, a w UE: *EU measures following the Russian invasion of Ukraine*, https://taxation-customs.ec.europa.eu/customs-4/international-affairs/eu-measures-following-russian-invasion-ukraine_en (dostęp: 15.03.2023).

[95] O. Bullough, *How Britain let Russia Hide Its Dirty Money*, https://www.theguardian.com/news/2018/may/25/how-britain-let-russia-hide-its-dirty-money (dostęp: 15.03.2023).

[96] J.K. Boyce, L. Ndikumana, *Kryzys w Ukrainie daje szansę na oczyszczenie brudnych pieniędzy*, https://wiadomosci.onet.pl/politico/kryzys-na-ukrainie-daje-szanse-na-oczyszczenie-brudnych-pieniedzy/zx0y3xf (dostęp: 28.02.2023).

[97] Ibidem.

[98] Ibidem.

Z kolei brytyjskie media piszą o finansowaniu wojny Putina w Ukrainie wartościami wypranymi w Wielkiej Brytanii (*assets laundered through the UK financing President Putin's war in Ukraine*)[99], których to doniesień władze brytyjskie nawet nie próbują dementować[100]. Wskazują jedynie na kroki legislacyjne, jakie podjęły lub zamierzają podjąć[101] (także we współpracy z innymi państwami[102]), zmierzające do egzekwowania sankcji nałożonych na Rosję i przeciwdziałania praniu pieniędzy. Faktem pozostaje jednak zarówno to, iż w Wielkiej Brytanii rosyjscy oligarchowie od lat deponują ogromne sumy (według brytyjskiego Biura Statystyk Narodowych rosyjskie inwestycje w tym kraju już na koniec 2016 r. szacowano na 25,5 mld funtów)[103], jak i to, że „brudne pieniądze" z Rosji nadal zasilają budżet tego kraju. Środki te niegdyś były transferowane z innych krajów, takich jak Cypr, Bahamy, albo z rajów finansowych (tj. Brytyjskich Wysp Dziewiczych, Kajmanów, Gibraltaru, Jersey i Guernsey). Pozwalało to na skuteczne utrudnianie wykrycia kraju, z którego faktycznie pochodzą[104]. Obecnie są one transferowane głównie przez kraje, które nie zdecydowały się objąć Rosji sankcjami, takie jak np. Armenia, Wietnam czy Chiny[105].

Pomimo zakazu oficjalnych kontaktów gospodarczych z Federacją Rosyjską wprowadzonego w wielu państwach, wynikającego z nałożonych na ten kraj sankcji, nadal wiele z nich utrzymuje jednak z Rosją relacje handlowe. Zazwyczaj nie odbywa się to w sposób jawny i legalny, a drogą interesów prowadzonych z firmami *off-shore*, przy współdziałaniu „najlepszych prawników, audytorów, bankierów i lobbystów na świecie", którzy pomagają rosyjskim oligarchom opracować

---

[99] R. Neate, *UK Failure to Tackle 'Dirty Money' Led to it 'Laundering Russia's War Funds'*, „The Guardian" 2022, 30.06, https://www.theguardian.com/business/2022/jun/30/uk-failure-to-tackle-dirty-money-led-to-it-laundering-russias-war-funds (dostęp: 25.02.2023).

[100] Por. *The Cost of Complacency: Illicit Finance and the War in Ukraine. Second Report of Session 2022–23 Report, Together With Formal Minutes Relating to the Report,* Published on 30 June 2022 by authority of the House of Commons, s. 4, 6. Do pobrania na stronie: https://publications.parliament.uk/pa/cm5803/cmselect/cmfaff/688/report.html (dostęp: 15.03.2023).

[101] *Government Response to the Cost of Complacency: Illicit Finance and the War in Ukraine. Second Report of Session 2022–23*, s. 1–12. Do pobrania na stronie: https://publications.parliament.uk/pa/cm5803/cmselect/cmfaff/688/report.html (dostęp: 15.03.2023).

[102] Warto wskazać, że od czasu wystąpienia Wielkiej Brytanii z Unii Europejskiej na mocy Umowy o wystąpieniu Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej z Unii Europejskiej i Europejskiej Wspólnoty Energii Atomowej (Dz. Urz. UE L z 2020 r., nr 29, s. 7), współpracę tego państwa z państwami członkowskimi UE w obszarze spraw karnych, niezależnie od konwencji, których stroną jest Wielka Brytania, normuje umowa o Handlu i Współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej z jednej strony a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej z drugiej – z 31.12.2020 r. Por. także: A. Grzelak, T. Ostropolski, P. Rakowski, *Uwarunkowania prawne i konsekwencje wyłączenia Zjednoczonego Królestwa ze współpracy w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (opt-out)*, „Europejski Przegląd Sądowy" 2013, nr 9, s. 11–19.

[103] O. Bullough, *How Britain Let Russia Hide Its Dirty Money*, https://www.theguardian.com/news/2018/may/25/how-britain-let-russia-hide-its-dirty-money (dostęp: 15.03.2023).

[104] Ibidem.

[105] *Rosyjscy cyberprzestępcy…*, op. cit. https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjscy-cyberprzestepcy-szukaja-nowych-sposobow-prania-pieniedzy-wszystko-przez-wojne (dostęp: 12.03.2023).

legalne sposoby ukrywania i „prania" swoich funduszy[106]. Do takich działań dochodziło zresztą już od wielu lat (także przed napaścią Rosji na Ukrainę) i dotyczyło też niejednego europejskiego państwa[107]. Aktualna sytuacja jedynie przyczyniła się do poszukiwania przez sprawców nowych metod i sposobów na ukrycie nielegalnie osiąganych korzyści majątkowych.

## JURYSDYKCJA W CYBERPRZESTRZENI I WALKA Z PRANIEM PIENIĘDZY

Poza trudnościami związanymi z samymi regulacjami dotyczącymi czynów bazowych, w tym określeniem oraz uregulowaniem cyberprzestępstw, pojawiają się także konkretne problemy związane ze ściganiem tych przestępstw (zarówno czynów bazowych, jak i prania pieniędzy), tudzież okolicznością, iż obejmują one terytorium niejednego państwa[108]. To z kolei rodzi problemy związane z jurysdykcją, najbardziej widoczne w odniesieniu do przestępstw popełnionych w cyberprzestrzeni. Zagadnienie to można zaś rozpatrywać na trzech płaszczyznach, tj.: ustawodawczej (legislacyjnej), wykonawczej i sądowej[109]. Mianem jurysdykcji zwykło się przy tym określać: „prawo państwa do wkraczania w sferę praw i obowiązków ludzi" lub też „prawo państwa do regulowania ich zachowania w sprawach niemających wyłącznie charakteru wewnętrznego (krajowego)"[110]. Zazwyczaj przyjmuje się, że jurysdykcja ma charakter terytorialny[111], czego wyrazem w polskim prawie karnym jest zasada terytorialności (art. 5 k.k.). Odstępstwa od niej przewidziano w art. 109–113 k.k. (zasady prawa karnego międzynarodowego). Jak dostrzeżono jednak, zastosowanie zasady terytorialności do „tego terytorialnego tworu, jakim jest cyberprzestrzeń"[112] może okazać się kłopotliwe. Wynika to ze specyficznej wielomiejscowości takich czynów. Wobec tego wysunięto niejedną propozycję rozwiązania sporów dotyczących jurysdykcji karnej w sprawach o przestępstwa

---

[106] BBC News, *Russian Oligarchs: Where Do They Hide Their 'Dark Money'?*, https://www.bbc.com/news/world-60608282 (dostęp: 15.03.2023).

[107] Szlaki „brudnych" środków wiodły m.in. przez Litwę, Łotwę, Estonię, Danię i Szwecję, a także przez Polskę, por. Haga (Reuters), *Europejskie kraje bałtyckie są zagrożone dalszym praniem brudnych pieniędzy przez Rosję* (raport Europolu), https://www.reuters.com/article/us-europe-moneylaundering-europol-idUSKCN1TE2K6; https://www.dw.com/en/how-ing-bank-in-poland-helped-russians-launder-money/a-55322399 (dostęp: 15.03.2023).

[108] O tym por. K. Góral, P. Opitek, *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora, cz. II*, „Prokuratura i Prawo" 2020, nr 6, s. 91–116.

[109] J. Czekalska, *Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych*, „Państwo i Prawo" 2004, nr 11, s. 74.

[110] J.H. Beale, *The Jurisdiction of a Sovereign State*, „Harvard Law Review (HLR)" 1923, t. 36, s. 241, za: M. Płachta, *Konflikty jurysdykcyjne w sprawach karnych: pojęcie, geneza i środki zaradcze*, „Prokuratura i Prawo" 2010, z. 11, s. 5.

[111] F.A. Mann, *The Doctrine of Jurisdiction in International Law*, „Recueil des Cours de l'Academie de droit international (RCADI)" 1964, t. 111, s. 9–162, za: M. Płachta, *Konflikty jurysdykcyjne…*, op. cit., s. 75.

[112] J. Czekalska, *Jurysdykcja w cyberprzestrzeni…*, op. cit., s. 75.

w cyberprzestrzeni[113]. Postulowano nawet uznanie cyberprzestrzeni za „czwartą przestrzeń", a także wprowadzenie wyjątku od zasady terytorialności na rzecz zasady narodowościowej[114]. Podzielając wątpliwości na temat trudności, jakie sprawia określenie jurysdykcji w sprawach o cyberprzestępstwa, nie wydaje się jednak, aby ostatnie z zaproponowanych było najlepszym rozwiązaniem (przynajmniej w świetle rodzimego prawa karnego, ze świadomością wszakże odmiennego podejścia do tej kwestii w innych systemach prawna karnego[115]). Nie wydaje się bowiem, by było konieczne odejście od tradycyjnie określanego miejsca czynu[116], pomimo niewątpliwej specyfiki przestępstw popełnionych w cyberprzestrzeni i okoliczności, w jakich do nich dochodzi (otwarta architektura, niezależność od miejsca, względna anonimowość etc. – jako cechy cyberprzestrzeni[117]). Oczywiste pozostaje przy tym, iż miejscem czynu w tym przypadku może być zarówno miejsce „fizycznego" umieszczenia hosta/ów i serwera/ów (infrastruktury), faktycznego przebywania sprawcy w czasie czynu, jak i miejsce, w którym nastąpił skutek (np. doszło do wykradzenia danych). Tym samym jurysdykcja państwa obejmuje sprawców przebywających na jego terytorium oraz wobec czynów popełnionych z wykorzystaniem lub przeciwko infrastrukturze znajdującej się na jego terytorium[118]. Konflikty na płaszczyźnie sądowej dotyczące takich przestępstw należy natomiast rozwiązywać tak, jak ma to miejsce w odniesieniu do wszystkich innych przestępstw wielomiejscowych, czyli na podstawie procedur postępowania karnego, zgodnie z zaakceptowanymi przez dane państwo porozumieniami międzynarodowymi[119]. Z kolei w odniesieniu do płaszczyzny ustawodawczej i zasady podwójnej karalności *in concreto* należy poprzestać na dotychczasowym sposobie określania miejsca/miejsc czynu/czynów. W przeciwnym wypadku należałoby raczej rozważyć ustanowienie jakiejś odrębnej zasady – umownie – „cyberterytorialności", która (być może) doprowadziłaby do konsensusu w zakresie ustalenia jednego miejsca czynu, zarazem jednak – co wysoce prawdopodobne – komplikując czynności podejmowane w postępowaniu karnym w sprawie o cyberprzestępstwo. Tych zaś jest niemało. Tematyce tej poświęcono zresztą sporo uwagi i opisano ją na łamach niejednego opracowania[120].

---

[113] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe.* Status quo *i perspektywy*, Warszawa 2020, s. 99–110.

[114] Obok Antarktyki, przestrzeni kosmicznej i otwartego morza – J. Czekalska, *Jurysdykcja w cyberprzestrzeni…*, op. cit., s. 74, 80–81.

[115] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe…*, op. cit., s. 99–101, 118–136.

[116] Zgodnie z art. 5 § 2 k.k.: „Czyn zabroniony uważa się za popełniony w miejscu, w którym sprawca działał lub zaniechał działania, do którego był obowiązany, albo gdzie skutek stanowiący znamię czynu zabronionego nastąpił lub według zamiaru sprawcy miał nastąpić".

[117] T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni…*, op. cit., s. 12.

[118] Ibidem, s. 24.

[119] Por. art. 22 Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728), której sygnatariuszami jest w sumie 67 państw, por. https://pl.frwiki.wiki/wiki/Convention_sur_la_cybercriminalit%C3%A9 (dostęp: 18.03.2023).

[120] Por. np. B. Nita-Światłowska, *Wymóg podwójnej karalności oraz zgody skazanego jako przesłanki przejęcia kary pozbawienia wolności do wykonania według konwencji strasburskiej o przekazywaniu osób skazanych*, „Europejski Przegląd Sądowy" 2019, nr 9, s. 4–12; R. Kierzynka, *Wzajemne uznawanie orzeczeń przepadku między państwami członkowskimi Unii Europejskiej*, „Prokuratura i Prawo" 2010, nr 9, s. 16–21; S. Steinborn, *Kolizje norm o międzynarodowej współpracy w sprawach karnych*

Wskazywano przy tym *expressis verbis* na zasadnicze przeszkody, jakie pojawiają się na drodze do „pełnego oraz powszechnego uznawania i wykonywania zagranicznych orzeczeń karnych", takie jak: suwerenność państwa, brak ekwiwalentności systemów prawnych, brak zaufania w stosunkach międzynarodowych oraz trudności wynikające z wewnętrznych systemów prawnych poszczególnych państw[121]. Przypominano również o możliwościach wyeliminowania tych trudności m.in. przez wyrażenie zgody przez państwa-strony porozumienia, zasadę wzajemności, proces unifikacji, procedurę *exequatur* czy stosowanie klauzuli porządku publicznego[122]. Nie może wobec tego dziwić zapatrywanie wyrażone w literaturze przedmiotu, iż: „zasada podwójnej przestępności czynu niejednokrotnie wręcz udaremnia współpracę" i „wobec różnic regulacji prawnych już samo definiowanie typów przestępstw w aktach prawa wspólnotowego lub unijnego nastręcza trudność"[123].

## PRZEMYT MIGRANTÓW I HANDEL LUDŹMI A ZWALCZANIE PRANIA PIENIĘDZY W ŚWIETLE DOKUMENTÓW FATF

Analizując zagadnienie współpracy międzynarodowej w zwalczaniu prania pieniędzy, tudzież odnosząc je do aspektów związanych z aktualnymi zagrożeniami, nie sposób wreszcie nie wspomnieć o jeszcze jednej kwestii, a mianowicie o przemycie migrantów. Zwraca na nie uwagę również Grupa Specjalna ds. Prania Pieniędzy[124]. Jak wskazuje FATF, przemyt migrantów ma z natury charakter transgraniczny, a przy tym nierzadko wiąże się z przewożeniem osób przez granicę w celu ich wykorzystywania. Zagrożeń płynących z przemytu migrantów i handlu ludźmi zatem, pomimo iż są to różne przestępstwa[125], nie sposób zupełnie oddzielić. Dotyczy to także perspektywy „prania" pochodzących z nich korzyści. Według danych Frontexu zyski z takiej działalności, poddawane „praniu", sięgają nawet 10 miliardów dolarów rocznie[126]. Z kolei handel ludźmi, jako czyn bazowy prania pieniędzy, chociaż *per se* z całą pewnością trudno uznać za nowe zjawisko, to jednak co do formy i metod popełnienia tego przestępstwa ulega zmianom[127]. Handel ludźmi, nie tylko w celach seksualnych, ale także w postaci np. handlu narządami, odbywa

---

*w zakresie zabezpieczenia mienia*, „Europejski Przegląd Sądowy" 2007, nr 4, s. 15–25. W kwestii zmiany terminologii i zastąpieniu pojęć: „państwo wzywające" i „państwo wezwane" określeniami: „państwo wydania" i „państwo wykonania" – Z. Barwina, *Zasada wzajemnego uznawania…*, op. cit., s. 157.

121 M. Aksamitowska-Kobos, *Wnioski sądów polskich…*, op. cit., s. 22.

122 Ibidem.

123 P. Hofmański, *Przyszłość ścigania…*, op. cit., s. 5.

124 Por. FATF, *Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling*, Paris 2022, s. 18–27. Dokument do pobrania ze strony: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Migrant-smuggling.html (dostęp: 15.02.2023).

125 Por. J. Jambor, *Pokrzywdzony – ofiara handlu ludźmi w procedurach dochodzeniowych i sądowych*, „Prokuratura i Prawo" 2022, nr 9, s. 42.

126 FATF, *Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling…*, op. cit., s. 18.

127 R. Mroczek, *Formy inicjacji procesowej w sprawach o przestępstwa handlu ludźmi*, „Prokuratura i Prawo" 2019, nr 2, s. 95–97.

się coraz częściej przy wykorzystaniu Internetu. Natomiast niezmiennie preferowaną formą „zapłaty" jest gotówka (52%), a następnie jej transport (i to dosłownie) między jurysdykcjami[128]. Popularne jest także wykorzystywanie w tym celu nieformalnych systemów transferu pieniędzy (*informal value transfer system*, IVTS), takich jak *hawala* i powtarzające się transakcje kartami przedpłaconymi poza miejscem zamieszkania posiadacza[129]. Jest to nieobojętne z punktu widzenia przeciwdziałania praniu pieniędzy i postępowania karnego prowadzonego w takich sprawach. Samej problematyce dotyczącej działań strategicznych oraz czynności operacyjnych prowadzonych w kooperacji międzynarodowej w sprawach o przestępstwo handlu ludźmi poświęcono odpowiednio dużo miejsca na łamach fachowej literatury[130]. Analiza trudności z tym związanych wykraczałaby przy tym poza ramy tego opracowania. Biorąc pod uwagę meritum, a zatem ów „finansowy komponent" (*financial component*) tych przestępstw, należałoby odwołać się do wniosków z raportu FATF dotyczącego problemu przemytu migrantów[131]. W ocenie tej organizacji, podstawowymi środkami służącymi współpracy międzynarodowej w zwalczaniu prania pieniędzy pochodzących z takich czynów są: rzetelne gromadzenie, analizowanie oraz wymiana informacji finansowych, a także skuteczne odzyskiwanie mienia[132].

## PODSUMOWANIE

Rekapitulując, zaprezentowane powyżej kwestie dowodzą niezbicie, że pranie pieniędzy jako proceder podlega stałym zmianom. Są one uwarunkowane zarówno bieżącą sytuacją panującą na świecie, w szczególności w sferze ekonomicznej i politycznej, jak i rozwojem nowoczesnych technologii. Dynamika życia społeczno-gospodarczego, a także bieżąca sytuacja polityczna stwarzają nowe możliwości dla pomysłowych sprawców prania pieniędzy, jednocześnie stawiając wyzwanie przed organami i instytucjami powołanymi do walki z nim.

Mając zaś na względzie fakt, iż przestępstwo prania pieniędzy przybiera zazwyczaj charakter transgraniczny i nierzadko wykracza poza obszar Unii Europejskiej, istotne stają działania prewencyjne podejmowane względem państw uznanych za stwarzających wysokie ryzyko pod kątem możliwości prania w nich pieniędzy, tudzież opracowanie zasad współpracy z krajami spoza struktur unijnych. Oczywiste pozostaje przy tym to, iż poza potrzebą opracowania regulacji prawnych w tym zakresie, konieczne jest również podejmowanie konkretnych działań prowadzonych w porozumieniu z tymi państwami. Nie sposób pominąć przy tym faktu, iż na etapie maskowania (nawarstwiania; *layering*) pranie pieniędzy jest popełniane nierzadko w jurysdykcjach, które, teoretycznie, nie nasuwają zastrzeżeń co do szczelności ich

---

[128] https://dxcompliance.com/money-laundering-risks-arising-from-migrant-smuggling/ (dostęp: 12.03.2023).

[129] FATF, *Money Laundering…*, op. cit., s. 20–24.

[130] Por. np. K. Galla-Podsiadło, W. Jakimko, M. Matyjewicz, T. Nowak, *Współpraca międzynarodowa w sprawach o handel ludźmi*, „Prokuratura i Prawo" 2022, nr 9, s. 170–229.

[131] FATF, *Money Laundering…*, op. cit., s. 7, 44–45.

[132] Ibidem, s. 34–35.

systemów finansowych. Nie oznacza to jednak, iż współpraca z takimi krajami pozostaje wolna od problemów. Nadal u ich źródła leży niejednokrotnie zasada podwójnej karalności, czego dowodzą chociażby opisane w opracowaniu trudności wynikające z transakcji kryptoaktywami, a także konsekwencje wojny na Ukrainie w zakresie transakcji handlowych. W odniesieniu do współpracy z państwami trzecimi może się ona okazać problematyczna zarówno na płaszczyźnie legislacyjnej, jak i sądowej. Wynika to z faktu, że państwa trzecie nie zawsze są skłonne do współpracy, powołując się na istnienie różnych przeszkód o charakterze formalnym lub faktycznym. Przykładem tego są państwa zaliczane do rajów podatkowych. Utrudniają one wykrycie śladów przepływu „brudnych" wartości majątkowych lub uniemożliwiają dostęp do informacji na ten temat. Ograniczają także skuteczność działań podejmowanych przez organy powołane do walki z tym zjawiskiem, w szczególności tzw. jednostki analityki finansowej (JAF) innych krajów. Bezdyskusyjne pozostaje przy tym to, iż transgraniczny charakter, jaki przeważnie przybiera proceder „prania", wymaga skoordynowanych działań, podejmowanych na podstawie wspólnie wypracowanych środków prawnych.

Na arenie międzynarodowej, obejmującej nie tylko państwa unijne, rolę strażnika standardów AML/CFT pełni w szczególności FATF. Opierając się na dokumentach opracowanych przez tę organizację, a także odnosząc się do aktualnych zagrożeń w zakresie prania pieniędzy, należy uznać, że skuteczność zwalczania tego procederu wymaga wzmocnienia współpracy dwustronnej i międzynarodowej zarówno między JAF (w tym za pośrednictwem Grupy Egmont), jak i organami ścigania oraz innymi organami właściwymi w zakresie wymiany informacji i świadczenia wzajemnej pomocy prawnej. Odnosi się to zwłaszcza do państw, które powołują się na regulacje krajowe, uniemożliwiając tym samym ujawnienie istotnych okoliczności czynów bazowych lub prania pieniędzy oraz wykrycie ich sprawców. Poza konieczną rezygnacją z tworzenia barier na drodze wykrywania przestępstw bazowych i ich związku z praniem nielegalnych korzyści majątkowych, niezbędne jest także zacieśnianie współpracy między państwami sąsiadującymi (współpracy granicznej) w celu wyeliminowania zagrożeń regionalnych, przede wszystkim odnoszących się do problemów migracyjnych. Wreszcie, uznając za newralgiczne cyberprzestępstwa jako czyny bazowe „prania", a także *cyberlaundering* jako formę popełnienia omawianego procederu, nieodzowne wydaje się także dążenie do wypracowania spójnych rozwiązań prawnych w tym zakresie. Powinny one obejmować nie tylko standardy określające zasady gromadzenia i przekazywania informacji o podejrzanych transakcjach, ale również regulacje umożliwiające skuteczne ściganie ich sprawców oraz wykonanie orzeczonych kar.

## BIBLIOGRAFIA


Aksamitowska-Kobos M., *Wnioski sądów polskich o wykonanie orzeczeń w sprawach karnych dotyczących kar o charakterze pieniężnym kierowane za granicę*, „Iustitia" 2015, nr 1.

Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, t. 8, z. 15.

Allen F., Gu X., Jagtiani J., *Fintech, Cryptocurrencies and CBDC: Financial Structural Transformation in China*, „Working Papers – Federal Reserve Bank of Philadelphia" 2022, vol. 22 (4).

Augustyniak B., w: *Kodeks postępowania karnego. Tom II. Komentarz aktualizowany*, red. D. Świecki, wyd. 6, Warszawa 2022.

B/A (KWP w Białymstoku), *Jak przestępcy wykorzystują pandemię*, „Policja 997" 2020, nr 182.

B/A, *Scams & Swindles: Phishing, Spoofing, ID Theft, Nigerian Advance Schemes, Investment Frauds, False Sweethearts: How to Recognize and Avoid Financial Rip-offs in the Internet Age*, wyd. I, Los Angeles 2006.

Balkowski R., *Bezpieczeństwo systemów teleinformatycznych – zmiany, trendy i zasady*, Warszawa 2018.

Banach-Gutierrez J., *Europejski wymiar sprawiedliwości w sprawach karnych. W kierunku ponadnarodowego systemu* sui generis*?*, Warszawa 2011.

Barwina Z., *Zasada wzajemnego uznawania w sprawach karnych*, Warszawa 2012.

Behan A., *Waluty wirtualne jako przedmiot przestępstwa*, Kraków 2022.

Brodowski L., *Zasada podwójnej karalności czynu w kontekście ekstradycji*, „Studia Prawnicze KUL" 2015, nr 1.

Czekalska J., *Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych*, „Państwo i Prawo" 2004, nr 11.

Dela P., *Teoria walki w cyberprzestrzeni*, Warszawa 2020.

European Union Agency for Criminal Justice Cooperation – „Eurojust", *Money laundering cases registered at Agency doubled in last 6 years according to Eurojust's new report z 20.10.2022 r.*, https://www.eurojust.europa.eu/news/money-laundering-cases-registered-agency-doubled-last-6-years-according-eurojusts-new-report.

Frąckowiak-Adamska A., Grzeszczak R., *Europejska przestrzeń sądowa*, Wrocław 2010.

Galla-Podsiadło K., Jakimko W., Matyjewicz M., Nowak T., *Współpraca międzynarodowa w sprawach o handel ludźmi*, „Prokuratura i Prawo" 2022, nr 9.

Gardocki L., *Podwójna przestępność czynu w prawie ekstradycyjnym*, w: *Problemy nauk penalnych. Prace ofiarowane Pani Profesor Oktawii Górniok*, Katowice 1996.

Gawłowicz I., Wasilewska M.A., *Międzynarodowa współpraca w walce z przestępczością (międzynarodowe trybunały, Interpol)*, Szczecin 2004.

Golonka A., *Prawnokarne zagadnienia przeciwdziałania wprowadzania do obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł*, Rzeszów 2008.

Golonka A., *Scamming*, w: *Przestępczość zorganizowana. Aspekty prawne kryminalno-kryminalistyczne*, red. P. Łabuz, I. Malinowska, M. Michalski, Warszawa 2022.

Góral K., Opitek P., *Analiza kryminalna transferów kryptowalutowych w pracy prokuratora, cz. II*, „Prokuratura i Prawo" 2020, nr 6.

Grzelak A., Kolowca I., *Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości Unii Europejskiej. Współpraca policyjna i sądowa w sprawach karnych. Dokumenty. Tom 1*, wyd. 1, Warszawa 2009.

Grzelak A., Ostropolski T., Rakowski P., *Uwarunkowania prawne i konsekwencje wyłączenia Zjednoczonego Królestwa ze współpracy w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (opt-out)*, „Europejski Przegląd Sądowy" 2013, nr 9.

Grzelak A., *Trzeci filar Unii Europejskiej. Instrumenty prawne*, Warszawa 2008.

Grzywacz J., *Pranie pieniędzy. Metody, raje podatkowe, zwalczanie*, Warszawa 2010.

Guberow P., *Techniki prania brudnych pieniędzy*, w: *Pranie brudnych pieniędzy*, red. J. Grzywacz, Warszawa 2005.
Hartikainen E.I., *The Nigerian Scam: Easy Money on the Internet, But For Whom?*, Michigan 2006.
Hofmański P., *Przyszłość ścigania karnego w Europie*, „Europejski Przegląd Sądowy" 2006, nr 12.
IEWG, *FIU-FinTech Cooperation and Associated Cybercrime Typologies and Risks*, Ottawa, July 2022.
Jambor J., *Pokrzywdzony – ofiara handlu ludźmi w procedurach dochodzeniowych i sądowych*, „Prokuratura i Prawo" 2022, nr 9.
Jankowski J., *Klauzula przeciwko unikaniu opodatkowania (GAAR). Przepisy materialnoprawne*, Warszawa 2022.
Jasiński W., *Pranie brudnych pieniędzy*, Warszawa 1998.
Kierzynka R., *Wzajemne uznawanie orzeczeń przepadku między państwami członkowskimi Unii Europejskiej*, „Prokuratura i Prawo" 2010, nr 9.
Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.
Kowalczyk M., *Ripple – czym jest i czy warto zainwestować?* (cykl: kryplowaluty z 11.10.2021 r.).
Krysztofiuk G., *Zasada wzajemnego uznawania orzeczeń w sprawach karnych w Traktacie Lizbońskim*, „Prokuratura i Prawo" 2011, nr 7.
Krysztofiuk G., *Perspektywy współpracy sądowej w sprawach karnych w Unii Europejskiej*, „Prokuratura i Prawo" 2015, nr 7–8.
Kuczyńska H., *Glosa do postanowienia Sądu Najwyższego z dnia 22 listopada 2011 r., sygn. IV KK 267/11*, „Prokuratura i Prawo" 2013, nr 3.
Kumar R., *Kidney Transplants and Scams: India's Troublesome Legacy*, New Delhi 2020.
Kuźniacki B., *Wymiana informacji podatkowych z innymi państwami. Nowa era stosowania prawa podatkowego w wymiarze międzynarodowym. Wymiana informacji o rachunkach finansowych, interpretacjach podatkowych oraz informacji o jednostkach z grupy (cz. 2)*, „Przegląd Podatkowy" 2017, nr 6.
Lach A., *Europejska pomoc prawna w sprawach karnych*, Toruń 2007.
Liwo M.A., *Współpraca transgraniczna Unii Europejskiej jako przejaw integracji narodów w zapewnieniu poczucia bezpieczeństwa*, „Przegląd Prawa Publicznego" 2013, nr 7–8.
Marek A., *Komentarz do Konwencji w sprawie prania dochodów pochodzących z przestępstwa, ich ujawniania, zajmowania i konfiskaty*, w: *Standardy prawne Rady Europy. Teksty i komentarz. Tom III – Prawo karne*, red. E. Zielińska, Warszawa 1997.
Maroń H., *Współpraca policyjna i sądowa w sprawach karnych wg projektu Konstytucji Europejskiej*, „Państwo i Prawo" 2007, nr 4.
McDonalds O., *Cryptocurrencies: Money, Trust and Regulation, Agenda Publishing*, Newcastle 2021.
Michalczuk C., *Współpraca prawna w sprawach karnych z „rajami podatkowymi"*, „Prokuratura i Prawo" 2010, nr 9.
Mika J.F., Mika M., *Istota rajów podatkowych*, w: *Raje podatkowe. Procedura należytej staranności, obowiązki w cenach transferowych*, red. J.F. Mika, Warszawa 2023.
Mroczek R., *Formy inicjacji procesowej w sprawach o przestępstwa handlu ludźmi*, „Prokuratura i Prawo" 2019, nr 2.
Nita-Światłowska B., *Wymóg podwójnej karalności oraz zgody skazanego jako przesłanki przejęcia kary pozbawienia wolności do wykonania według konwencji strasburskiej o przekazywaniu osób skazanych*, „Europejski Przegląd Sądowy" 2019, nr 9.
Obczyński R., w: *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, red. W. Kapica, Warszawa 2020.
Ocieczek G., Opitek P., *Praktyczne aspekty zwalczania przestępczości narkotykowej dokonywanej w „świecie realnym" i cyberprzestrzeni*, „Prokuratura i Prawo" 2022, nr 7–8.

Online African Organized Crime from Surface to Darkweb, Raport analityczny UE i INTERPOL-u, 2020.

Opitek P., *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12.

Płachta M., *Konflikty jurysdykcyjne w sprawach karnych: pojęcie, geneza i środki zaradcze*, „Prokuratura i Prawo" 2010, z. 11.

Płachta M., *Uznawanie i wykonywanie zagranicznych orzeczeń karnych. Zagadnienia podstawowe*, „Państwo i Prawo" 1985, nr 3.

Pszczółkowski S., *Zagadnienie podwójnego opodatkowania w stosunkach międzynarodowych* (rozprawa doktorska przyjęta przez Radę Wydziału Prawa UW uchwałą z dnia 1.05.1925 r.), UW, Warszawa 1928.

Riley J., *The Current Status of Cryptocurrency Regulation in China and Its Effect around the World*, „China and WTO Review" 2021, vol. 7 (1).

Rojszczak M., *Cyberbezpieczeństwo 2.0: w poszukiwaniu nowych ram ochrony cyberprzestrzeni*, w: *Cyberbezpieczeństwo*, red. C. Banasiński, J.M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, M. Rojszczak, K. Waćkowski, Warszawa 2020.

Steinborn S., w: *Europejskie prawo karne*, red. A. Grzelak, M. Królikowski, A. Sakowicz, wyd. I, Warszawa 2012.

Steinborn S., *Kolizje norm o międzynarodowej współpracy w sprawach karnych w zakresie zabezpieczenia mienia*, „Europejski Przegląd Sądowy" 2007, nr 4.

Szumski A., *Współpraca międzynarodowa w zwalczaniu przestępczości zorganizowanej na obszarach dawnych konfliktów etnicznych na przykładzie misji EULEX Kosowo*, „Wschodnioznawstwo" 2016, nr 10.

Szwarc A.J., Długosz J., *Unijne instrumenty współdziałania państw w sprawach karnych*, „Edukacja Prawnicza" 2011, nr 3.

Weerth C., *INTERPOL on COVID-19: COVID-19 Crime and Fraud Alert*, „Technical Raport" 2020, April.

Weerth C., *INTERPOL on COVID-19: Urgent Safety alert – Results of the 2020 Fake Medicine and Medicine Products Operation PANGEA XIII*, „Technical Raport" 2020, March.

Wójcik J.W., *Pranie pieniędzy. Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Warszawa 2002.

Wójcik J.W., *Przeciwdziałanie praniu pieniędzy*, Kraków 2004.

Worona J., *Cyberprzestrzeń a prawo międzynarodowe.* Status quo *i perspektywy*, Warszawa 2020.

Wyrozumska A., *Umowy międzynarodowe. Teoria i praktyka*, Warszawa 2007.

Zaród M., *Aktorzy-sieci w kolektywach hakerskich*, Warszawa 2018.

Zaród M., *Hakerzy i kolektywy hakerskie w Polsce. Od operacjonalizacji do laboratoriów i stref wymiany*, „Przegląd Socjologiczny" 2017, t. 1, z. 224.

Zych J., *Teleinformatyka dla bezpieczeństwa*, Poznań 2019.

**Cytuj jako:**

Golonka A., *Współpraca z krajami trzecimi w zwalczaniu prania pieniędzy w obliczu współczesnych wyzwań*, „Ius Novum" 2023 (17) nr 4, s. 16–39. DOI: 10.26399/iusnovum.v17.4.2023.27/a.golonka