sciendo

Ius Novum

2023, vol. 17, no. 4, pp. 15–39

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

ANNA GOLONKA*

DOI: 10.2478/in-2023-0027

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 highlight the difficulties that, in the current global situation, are posed by cooperation with third countries, i.e., those that are not members of the European Union. The analysis covers several thematic areas that are of key importance in this regard (using the formal dogmatic method). The specificity of the regulations in force in other countries was also indicated, particularly in the context of modern technologies and threats of cyber-laundering (incorporating elements of the legal and comparative method). As a result, conclusions were drawn regarding the challenges that the fight against laundering raises on the international arena, extending beyond the structures of the EU. The conclusion suggests directions for 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

* LLD hab., Professor of the University of Rzeszów – head of the Department of Criminal Law at the Institute of Legal Sciences at the University of Rzeszów (Poland), e-mail: agolonka@ur.edu.pl, ORCID: 0000-0002-0199-2203.

INTRODUCTION

Money laundering is one of the most serious economic crimes, both in terms of economic effects and its global scale.[1] Combating this practice includes not only penalising the crime referred to in Article 299 of the Polish Criminal Code,[2] but also anti-money laundering activities.[3] In the Polish legal system, the basic legal act regulating this matter is the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (AML/CTF Act (*Anti-Money Laundering/Counter Terrorist Financing*)).[4] Due to the cross-border nature of money laundering, which is often associated with its complex nature,[5] the fight against money laundering at a transnational level is of particular importance. In this regard, the activities undertaken for years by EU institutions, which monitor the areas and scale of threats related to this phenomenon, are invaluable. In addition to preventive activities, the core of which, in the case of European Union Member States,[6] is undoubtedly determined by EU AML regulations, specific activities related to strategic and operational efforts are crucial. Currently, threats in this regard primarily arise from the political situation in the world, including ongoing armed conflicts, economic problems (significantly influenced by the Covid-19 pandemic), and the widespread digitisation of social and economic life. These issues were the incentive to consider the implications of modern challenges for international cooperation in the fight against money laundering. This issue is of particular importance in relation to the relationship with so-called third countries.[7]

---

[1] It is estimated that the world economy loses about 2 to 5% of the world's GDP annually due to money laundering, i.e. about EUR 1.87 trillion – cf. European Union Agency for Criminal Justice Cooperation (Eurojust), *Money laundering cases registered at Agency doubled in the last 6 years according to Eurojust's new report* of 20.10.2022, at: https://www.eurojust.europa.eu/news/money-laundering-cases-registered-agency-doubled-last-6-years-according-eurojusts-new-report [accessed on 7 March 2023].

[2] Criminal Code of 6 June 1997 (consolidated text Journal of Laws of 2022, item 1138, as amended).

[3] It should be noted that national and international regulations on anti-money laundering also cover anti-terrorist financing (AML/CFT). In this study, issues related to combating the financing of terrorism will be omitted.

[4] AML/CFT Act of 1 March 2018 (consolidated text Journal of Laws of 2022, item 593, as amended).

[5] It is most often assumed that money laundering in the 'model' approach proposed by the Financial Action Task Force (FATF) proceeds in three stages, i.e.: placement, layering and legitimisation (integration) – cf. Golonka, A., *Prawnokarne zagadnienia przeciwdziałania wprowadzania do obrotu wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł*, Rzeszów, 2008, pp. 28–44: https://www.iaml.com.pl/wiedza/etapy-prania-pieniedzy/ [accessed on 15 February 2023]. Sometimes, an additional phase preceding the above-mentioned is also indicated – cf. e.g.: Guberow, P., 'Techniki prania brudnych pieniędzy', in: Grzywacz, J. (ed.), *Pranie brudnych pieniędzy*, Warszawa, 2005, p. 24.

[6] On the draft EU amendment and the 'AML package' – cf. https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en [accessed on 19 February 2023]. This issue is so extensive that its exhaustive discussion in the present article is not possible and it is analysed in a separate study *Unijny projekt 'pakietu AML' – reforma czy rewolucja w zakresie przeciwdziałania praniu pieniędzy.*

[7] Accordingly Article 2(18) of the draft of /Regulation AML/CFT: 'third country means any jurisdiction, independent state or autonomous territory that is not part of the European Union but that has its own AML/CFT legislation or enforcement regime.'

This term includes both countries which, for various reasons, are considered conducive to the discussed practice (the so-called high-risk countries[8]), as well as others that remain outside the EU structures. In this case, the context of the current political, economic, and social situation in the world is also significant. It seems equally important to take into account the fact that in the era of widespread digitisation, the perpetrators of crimes often limit their activities to cyberspace only.[9] A separate issue is the need to ensure security in cyberspace. Combating money laundering in cyberspace has become one of the priority objectives of the European Union and organisations established to combat money laundering.[10] Significant difficulties arise at both the level of applying the law and its implementation. This study will be devoted to discussing these issues.

LEGAL BASES FOR INTERNATIONAL COOPERATION WITH THIRD COUNTRIES IN THE FIELD OF COMBATING THE MONEY LAUNDERING CRIME

In the vast majority of cases money laundering has a supranational character; therefore, its effective combat is possible only with efficient and well-coordinated cooperation between states. International cooperation in criminal matters regardless of the category of criminal acts to which it refers, inherently includes 'procedures developed in contacts between states in connection with their administration of justice in criminal matters'.[11] As such, it is based on rules that ensure these procedures are respected. The most important are the principle of reciprocity and

---

[8] Under Article 9 of Directive 2015/849, the term 'high-risk third countries' means: 'third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes'. In turn, the Act of 1 March 2018, AML/CFT, requires this term to include: each country identified 'based on information from reliable sources, including reports on the evaluation of national systems for counteracting money laundering and financing of terrorism carried out by the Special Group for Counteracting Money Laundering Money Laundering (FATF) and bodies or organisations related to it, as not having an effective anti-money laundering or countering the financing of terrorism system or having significant deficiencies in the anti-money laundering or countering the financing of terrorism system', recognising that it is 'in particular a third country identified by the European Commission in a delegated act adopted under Article 9 of Directive 2015/849' (Article 2(2)(13) of the AML/CFT Act).

[9] Cyberspace is: 'the space of human activity with the use of electronic devices for the production, storage, transmission, processing of and access to information' – cf. Dela, P., *Teoria walki w cyberprzestrzeni*, Warszawa, 2020, p. 35.

[10] Rojszczak, M., 'Cyberbezpieczeństwo 2.0: w poszukiwaniu nowych ram ochrony cyberprzestrzeni', in: Banasiński, C., Rojszczak, M., (eds), *Cyberbezpieczeństwo*, Warszawa, 2020, pp. 323–339; Aleksandrowicz, T.R., 'Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego', *Przegląd Bezpieczeństwa Wewnętrznego*. On the topic of the national 'cybersecurity' strategy – see *Strategia Cyberbezpieczeństwa RP na lata 2019–2024*, at: https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [accessed on 1 March 2023]; *The Central Bureau for Combating Cybercrime will be established*; at: https://www.gov.pl/web/mswia/powstanie-centralne-biuro-zwalczania-cyberprzestepczosci as well as at: https://cbzc.policja.gov.pl/bzc/aktualnosci/92,Ruszyl-proces-doboru-do-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html [accessed on 3 January 2023].

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

the principle of double criminality.[12] The literature also indicates the validity of other principles, including those constituting a kind of development of the former, i.e. the principle of reciprocity.[13] Much has been written about the difficulties that may arise with respect to the principles of reciprocity and double criminality. In the pages of many scientific studies, they have been presented both in a broader aspect, i.e., regarding international cooperation in criminal matters in general,[14] and in a narrower aspect – covering the fight against economic crime.[15] Some of the dilemmas already described in the literature, when related to money laundering, take on a new dimension. All the more so because it often involves 'the need for joint action of the judicial authorities of three or four countries, each of which belongs to a different circle and is entangled in networks of different obligations and agreements.'[16]

Bi- and multilateral agreements between states (that are international Conventions) create the legal foundations of international cooperation in combating organised crime, in particular related to money laundering.[17] From the perspective of the subject discussed, the most important conventions, to which Poland is also a party, are undoubtedly: the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, signed in Strasbourg on 8 November 1990,[18] and the Council of Europe Convention on Laundering, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, made in Warsaw on 16 May 2005 (hereinafter referred to as the 'Warsaw Convention'),[19] and in a broader

---

[12] Ibidem, pp. 43–84; Płachta, M., 'Uznawanie i wykonywanie zagranicznych orzeczeń karnych. Zagadnienia podstawowe', *Państwo i Prawo*, 1985, No. 3, pp. 88–89; Banach-Gutierrez, J., *Europejski wymiar sprawiedliwości w sprawach karnych. W kierunku ponadnarodowego systemu sui generis?*, Warszawa, 2011, pp. 156–208; Krysztofiuk, G., 'Zasada wzajemnego uznawania orzeczeń w sprawach karnych w Traktacie Lizbońskim', *Prokuratura i Prawo*, 2011, No. 7, p. 11; Szwarc, A.J., Długosz, J., 'Unijne instrumenty współdziałania państw w sprawach karnych', *Edukacja Prawnicza*, 2011, No. 3, pp. 31–34; Brodowski, L., 'Zasada podwójnej karalności czynu w kontekście ekstradycji', *Studia Prawnicze KUL*, 2015, No. 1, pp. 31–58.

[13] Steinborn, S., in: Grzelak, A., Królikowski, M., Sakowicz, A. (eds), *Europejskie prawo karne*, 1st ed., Warszawa, 2012, pp. 51–90.

[14] Krysztofiuk, G., 'Perspektywy współpracy sądowej w sprawach karnych w Unii Europejskiej', *Prokuratura i Prawo*, 2015, No. 7–8, pp. 186–205; Hofmański, P., 'Przyszłość ścigania karnego w Europie', *Europejski Przegląd Sądowy*, 2006, No. 12, pp. 4–11.

[15] Hofmański, P., 'Przyszłość ścigania…', op. cit., p. 5; Szumski, A., 'Współpraca międzynarodowa w zwalczaniu przestępczości zorganizowanej na obszarach dawnych konfliktów etnicznych na przykładzie misji EULEX Kosowo', *Wschodnioznawstwo*, 2016, No. 10, pp. 93–100; Gawłowicz, I., Wasilewska, M.A., *Międzynarodowa współpraca w walce z przestępczością (międzynarodowe trybunały, Interpol)*, Szczecin, 2004, pp. 27–36.

[16] Hofmański, P., 'Przyszłość ścigania…', op. cit., p. 5.

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

[18] Journal of Laws of 2003, No. 46, item 394. Marek, A., 'Komentarz do Konwencji w sprawie prania dochodów pochodzących z przestępstwa, ich ujawniania, zajmowania i konfiskaty', in: Zielińska, E. (ed.), *Standardy prawne Rady Europy. Teksty i komentarz. Tom III – Prawo karne*, Warszawa, 1997, pp. 561–568.

[19] Journal of Laws of 2008, No. 165, item 1028 with the Amendment to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, made in Warsaw on 16 May 2005, adopted in Strasbourg on 22 October 2014 (Polish edition: Journal of Laws of 2018, item 1328).

aspect: the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988,[20] European Convention of 20 April 1959 on Mutual Assistance in Criminal Matters[21] (as amended by the Second Additional Protocol[22]), Convention on the Transfer of Sentenced Persons, Strasbourg, 21 March 1983[23] together with the Additional Protocol of 18 December 1997[24] or the Schengen Agreement of 19 June 1990 with the Implementing Convention (SIS II),[25] extending the scope of legal aid.[26] At this point, they can only be mentioned, as the essence of this part of the study is mainly to show the real difficulties in international cooperation with third countries in the context of the current threats of 'laundering'. Similarly, it is appropriate to recall the initiatives taken for many years by international organisations established to combat it, of which our country is also a member. These include in particular: the Financial Action Task Force (FATF),[27] the Egmont Group,[28] and the Moneyval Committee.[29] Their role in this regard cannot be overestimated, as well as the fact that their documents, which contain analyses of trends in 'laundering' methods, indicate the areas and institutions most exposed to participation in practice and thus set out the directions of cooperation between countries that are members of these organisations. Currently, which should not come as a surprise, threats in this respect primarily result from the political situation prevailing in the world, including ongoing armed conflicts, economic problems (also caused by the Covid-19 pandemic), and finally from the widespread digitisation of social and economic life. The activities of these institutions are of key importance from the perspective of international dialogue, the result of which is the

---

[20] Journal of Laws of 1995, No. 15, item 69.

[21] Journal of Laws of 1999, No. 76, item 854.

[22] Journal of Laws of 2004, No. 139, item 1476.

[23] Journal of Laws of 1995, No. 51, item 279.

[24] Journal of Laws of 2000, No. 43, item 490.

[25] Act of 24 August 2007, on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System (Journal of Laws of 2021, item 1041, as amended) and changes in force as of 1 January 2023. (Journal of Laws of 2022, item 2642).

[26] Aksamitowska-Kobos, M., 'Wnioski sądów polskich o wykonanie orzeczeń w sprawach karnych dotyczących kar o charakterze pieniężnym kierowane za granicę', *Iustitia*, 2015, No. 1, p. 29.

[27] The Financial Action Task Force (FATF) was established during the G-7 summit in Paris in 1989. Currently, 39 countries are members (including the Russian Federation, suspended from 24 February 2023). Since 2007, the FATF has covered 125 countries with the AML/CFT verification procedure. More (including 40 FATF Recommendations) at: https://www.fatf-gafi.org/en/home.html [accessed on 22 February 2023].

[28] Information about the organisation, its goals, and current reports as well as the strategy for 2022–2027 on the official website of the Egmont Group: https://egmontgroup.org/ [accessed on 22 February 2023]. See also: Grzywacz, J., *Pranie pieniędzy. Metody, raje podatkowe, zwalczanie*, Warszawa, 2010, pp. 160–161.

[29] The Committee of Experts for the Evaluation of Anti-Money Laundering and Terrorist Financing Systems (Moneyval) was established in 1997, and is a permanent monitoring body of the Council of Europe, tasked with assessing compliance with the core international AML/CFT standards and the effectiveness of their implementation, and making recommendations to national authorities on necessary improvements to their systems. More at: https://www.coe.int/en/web/moneyval [accessed on 22 February 2023]. See also: Wójcik, J.W., *Pranie pieniędzy. Kryminologiczna i kryminalistyczna ocena transakcji podejrzanych*, Warszawa, 2002, p. 133.

development of coherent legal solutions in the field of money laundering. However, there are still many areas that, from the perspective of the discussed practice, require specific actions or the development of such solutions at the international level that will contribute to improving the effectiveness of prosecuting the perpetrators of this cross-border crime. To a large extent, this is due to the participation of high-risk countries in it. It should also be pointed out that difficulties in international cooperation with third countries in the field of combating money laundering are caused not so much by the crime, which, as a *delictum iuris gentium* (a crime under the law of nations), is usually covered by relevant bilateral or multilateral agreements, as by its predicate acts.

THE PROBLEM OF PREDICATE ACTS IN THE CONTEXT OF DIFFICULTIES IN COOPERATION WITH THIRD COUNTRIES IN COMBATING MONEY LAUNDERING

The predicate crimes, also called basic or primary acts of money laundering,[30] are, in fact, offences or misdemeanours from which financial benefits are derived, which are then introduced into legal circulation.[31] Predicate offences present many difficulties from both a dogmatic and a practical point of view. The reason for this is not only the need to demonstrate the connection of such acts with the dealings of 'laundering', but sometimes also these acts *per se*. This applies, for example, to issues related to determining the place and manner of their commission, their status in the legal order of a given country, the characteristics of the causative act, or even the circumstances of their commission. They become particularly debatable in the face of current threats and their presentation through the prism of the principle of double criminality already mentioned in this study. Therefore, although this issue itself is certainly not a novelty, having been subject to in-depth scientific research almost a century ago,[32] it deserves special attention in the context of basic acts of money laundering. At the same time, it is worth pointing out, as aptly stated in the literature, that:

> 'The concept of double criminality should be understood broadly, which means that when examining the fulfilment of the condition of double criminality, one should not only refer to the content of the provision of the Polish criminal act, which could correspond to the law of a foreign state, but also to the applicable interpretation relating to the scope of application of this provision in the Polish legal system. It is necessary to assess the whole factual situation (…).'[33]

As a result, it was also concluded that:

---

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

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

[32] Cf. e.g. Pszczółkowski, S., *Zagadnienie podwójnego opodatkowania w stosunkach międzynarodowych*, (doctoral dissertation adopted by the Council of the Faculty of Law of the University of Warsaw by a resolution of 1 May 1925), Warszawa, 1928.

[33] Cf. decisions of the Supreme Court of 22 November 2011, IV KK 267/11, OSNKW, 2012, No. 3, item 24.

> 'the concept of double criminality should have different meanings depending on whether we are talking about meeting this condition in an abstract situation – i.e., when a given behaviour is a behaviour prohibited by law in both countries (the so-called double criminality *in abstracto*) or we are investigating the possibility of charging the perpetrator with a given crime in a specific factual situation, which can only take place after transferring a specific behaviour to Polish law (double criminality *in concreto*).'[34]

In the first scope, i.e. in relation to the problem of the punishability of an act in a given legal order, fiscal crimes, including tax crimes, are particularly problematic. This is because the criminalisation of such acts is primarily justified by the need to protect the financial interest of a given state against the depletion of public law liabilities or exposure to them (using the nomenclature adopted in the Polish Fiscal Penal Code[35]). The tax law even mentions the phenomenon of international tax competition. It has been stated that:

> 'It is at the root of the behaviour of some countries that, by modifying existing legislation, try to reduce the financial burden imposed in their country on foreign investors, which is to cause greater flow of capital and thus increase the investment rate.'[36]

Issues related to international cooperation in the field of tax law, including the exchange of information between countries,[37] supported by relevant regulations[38] or aspects of the legality of tax avoidance,[39] have already been the subject of separate studies. At this point, it is worth noting that the particularly problematic aspect in this respect is international cooperation with countries considered the so-called 'tax havens'. A financial haven, also known as a tax oasis, asylum, or *offshore* jurisdiction,[40] is considered to be: 'an area where there is a legal system that allows foreign entities to reduce the tax burden in their home countries.'[41] Cooperation with such countries raises difficulties resulting from, among others, the lack of tax transparency towards other countries and relevant state institutions, the lack of willingness to undertake it regarding national, restrictive regulations regarding the protection of secrets (e.g.,

---

[34] Ibidem, and Kuczyńska, H., 'Glosa do postanowienia Sądu Najwyższego z dnia 22 listopada 2011 r., sygn. IV KK 267/11', *Prokuratura i Prawo*, 2013, No. 3, p. 171, as well as: Gardocki, L., 'Podwójna przestępność czynu w prawie ekstradycyjnym', in: *Problemy nauk karnych. Prace przekazane Profesorowi Oktawii Górniok*, Katowice, 1996, pp. 70–72.

[35] Article 53 §§ 26 and 26a of the Fiscal Penal Code, as consolidated text Journal of Laws of 2022, item 859 as amended.

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

[37] Kuźniacki, B., 'Wymiana informacji podatkowych z innymi krajami. Nowa era stosowania prawa podatkowego w wymiarze międzynarodowym. Wymiana informacji o rachunkach finansowych, interpretacjach podatkowych oraz informacjach o podmiotach grupy kapitałowej (część 2)', *Przegląd Podatkowy*, 2017, No. 6, pp. 17–30.

[38] Act of 9 March 2017 on the exchange of tax information with other countries (consolidated text, Journal of Laws of 2023, item 241).

[39] Jankowski, J., *Klauzula przeciwko unikaniu opodatkowania (GAAR). Przepisy materialnoprawne*, Warszawa, 2022, pp. 21–22; on 'international tax planning' (i.e. the use of legal mechanisms to reduce or eliminate taxation of income or wealth, the accumulation of income through the appropriate use of tax havens' – cf. Grzywacz, J., *Pranie pieniędzy. Metody…*, op. cit., p. 57.

[40] Grzywacz, J., *Pranie pieniędzy. Metody…*, op. cit., p. 51.

[41] Ibidem, p. 52.

Hong Kong, Cayman Islands), the use of low tax rates, liberal regulations defining the principles of doing business, etc.[42] Countries-financial havens, although they are most often parties to international conventions – in particular those mentioned above, due to reservations made to them,[43] often make cooperation undertaken on their basis practically impossible. It is also worth recalling that those countries that are not considered tax havens, in the light of either FATF lists or documents issued by other domestic[44] and foreign institutions,[45] also introduce restrictive regulations, e.g., regarding protection of banking secrecy or the rules for transferring certain information (e.g., the United States, Switzerland). Therefore, they make it difficult for other countries to cooperate with them in cases involving suspected money laundering.

CYBER-LAUNDERING AS A CHALLENGE FOR INTERNATIONAL COOPERATION IN THE FIGHT AGAINST THIS PHENOMENON

When analysing aspects related to current threats and considering them in the context of double criminality, it would be impossible not to mention cyber-laundering, as well as other crimes committed in cyberspace, which may also be the predicate acts of 'laundering'. They take the form of *cybercrimes* or *cyber-enabled crimes*,[46] i.e., crimes committed using electronic means of communication (headed by the

---

[42] Mika, J.F., Mika, M., 'Istota rajów podatkowych', in: Mika, J.F. (ed.), *Raje podatkowe. Procedura należytej staranności, obowiązki w cenach transferowych*, Warszawa, 2023, pp. 3, 13–15.

[43] For example, the Strasbourg Convention of 1990 on laundering, disclosure, seizure, and confiscation of the proceeds of crime on refusal to execute requests in the absence of dual criminality for predicate offenses for money laundering (Andorra, Netherlands Antilles, Aruba, Monaco); limiting the use of information to the proceeding in which the request was made (Andorra, Netherlands Antilles, Aruba, Liechtenstein, Monaco); execution of the request only following the national law of a given country – 'with respect for constitutional principles' and 'basic legal concepts' (Andorra, Netherlands Antilles, Aruba, Liechtenstein, Monaco, Isle of Man, Guernsey); refusal to execute the request if it is possible to classify the crime underlying the request as a tax or customs act (Netherlands Antilles, Aruba), cf. Michalczuk, C., 'Współpraca prawna w sprawach karnych z »rajami podatkowymi«', *Prokuratura i Prawo*, 2010, No. 9, pp. 138–139.

[44] Notice of the Minister of Finance on the announcement of the list of countries and territories indicated in the EU list of non-cooperative jurisdictions for tax purposes adopted by the Council of the European Union, which have not been included in the list of countries and territories applying harmful tax competition issued based on the provisions on personal income tax and regulations on corporate income tax, and the date of adoption of this list by the Council of the European Union of 10 March 2022, MP item 341, and also: Mika, J.F., Mika, M., 'Istota rajów podatkowych…', op. cit., pp. 13–14.

[45] Cf. documents from the meeting of the Economic and Financial Affairs Council on the EU list of non-cooperative jurisdictions of 14 February 2023, at: 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/ [accessed on 14 March 2023].

[46] On the subject of a narrow and broad approach to cybercrime – see: INTERPOL, *Online African Organized Crime from Surface to Darkweb. Analytical Report*, 2020, p. 12.

Nigerian scam[47]). In practice, they may include several very diverse acts in terms of nature and course. However, various forms and methods of online fraud (*fraud, scam, phishing, spoofing, pharming, etc.*)[48] remain the most frequently committed cybercrimes, from which the benefits are derived and subsequently introduced into legal circulation. This is confirmed in the reports of institutions established to combat money laundering, both domestic[49] and foreign.[50] There should be no doubt that the global situation related to the Covid-19 pandemic,[51] has contributed to a significant increase in the number of scams or frauds[52] on the Internet.[53] Suffice it to say that in the first months of 2020, Interpol sent an Urgent Safety Alert to the Police of all (then-194) member countries, containing a warning about the increased risk of *ransomware attacks*,[54] new techniques, and ways of cybercriminals' operation.[55] Under the auspices of Interpol, 'Operation Pangea XIII' was also carried out in 2020, involving the state services of 90 countries.[56] It was aimed at organised

---

[47] A Nigerian scam (also known as an African scam, *Nigerian scam*, or '419 scam') is: 'a type of fraud involving persuading the victim to transfer money to one of the African countries (originally Nigeria) to obtain a large benefit' – cf.: Balkowski, R., *Bezpieczeństwo systemów teleinformatycznych – zmiany, trendy i zasady*, Warszawa, 2018, p. 9, as well as an example of 'laundering' with the use of '419 scam' – Hartikainen, E.I., *The Nigerian Scam: easy money on the Internet, but for whom?*, Michigan, 2006, pp. 1–2, 4–5.

[48] *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*, 1st ed., Los Angeles, 2006, pp. 43–244, and also: Kosiński, J., *Paradygmaty cyberprzestępczości*, Warszawa, 2015, pp. 126–131.

[49] *Report of the General Inspector of Financial Information on the implementation of the Act of 1 March 2018 on counteracting money laundering and financing terrorism in 2021*, Warsaw, March 2022. The document can be downloaded at: https://www.gov.pl/web/finanse/sprawozdania-roczne-z-dzialalnosci-generalnego-inspektora-informacji-finansowej [accessed on 26 September 2023].

[50] See IEWG, *FIU-FinTech Cooperation and Associated Cybercrime Typologies and Risks*, Ottawa, July 2022, pp. 35–37. The document can be downloaded from the Egmont website: https://egmontgroup.org/ [accessed on 3 March 2023]; European Union Agency for Criminal Justice Cooperation (Eurojust), *Money laundering cases registered at Agency doubled in the last 6 years according to Eurojust's new report* of 20 October 2022, pp. 6, 39.

[51] KWP w Białymstoku, 'Jak przestępcy wykorzystują pandemię', *Policja997*, 2020, No. 182, pp. 47–48.

[52] On the differences between *fraud* and *scam* – cf. Golonka, A., 'Scamming', in: Łabuz, P., Malinowska, I., Michalski, M. (eds), *Przestępczość zorganizowana. Aspekty prawne kryminalno-kryminalistyczne*, Warszawa, 2022, pp. 290–303.

[53] Weerth, C., 'INTERPOL on COVID-19: COVID-19 Crime and Fraud Alert', *Technical Report*, April 2020, pp. 1–4. DOI: 10.13140/RG.2.2.33650.25282.

[54] Current *Ransomware* Threat – cf. SonicWall, *2022 SonicWall Cyber Threat Report*, intro. by Conner, B., pp. 12–20, available at: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf. [accessed on 24 November 2023].

[55] Terminology concerning the perpetrators of cybercrimes (hackers and crackers) – cf. Zaród, M., 'Hakerzy i kolektywy hakerskie w Polsce. Od operacjonalizacji do laboratoriów i stref wymiany', *Studia Socjologiczne*, 2017, Vol. 1, No. 224, pp. 227–228, as well as: idem, *Aktorzy-sieci w kolektywach hakerskich*, pp. 50, 54 (PhD dissertation – Institute Sociologii UW, Warszawa, 2018. To be downloaded from the repository at: https://depotuw.ceon.pl/handle/it e m/2909 [accessed on 26 February 2023].

[56] Weerth, C., 'INTERPOL on COVID-19: Urgent Safety alert – Results of the 2020 fake medicine and medicine products operation PANGEA XIII', *Technical Report*, March 2020, pp. 1–4. DOI: 10.13140/RG.2.2.13950.95040.

criminal groups conducting illegal activity in the field of online trading in drugs and *para-pharmaceuticals*. As a result, 121 people were arrested around the world and actions were taken to secure property worth a total of over 14 million dollars.[57]

The money of laundered benefits also comes from sexual cybercrime (e.g., *sextortion*),[58] various forms of human trafficking on the Internet,[59] trafficking in drugs and other intoxicants on the *darknet*,[60] trafficking in organs, etc.[61] This is just a snippet of the many crimes that take place in *cyberspace* – from those committed using online and mobile financial services (including online and mobile banking) or through crowdfunding platforms, to crimes increasingly committed using virtual assets (VA).[62] It is even indicated in the literature that the use of virtual currencies to support illegal activity, including money laundering, is currently one of the most dangerous phenomena for the financial systems of individual countries[63] and for the entire global community.[64]

CRYPTO-ASSETS AS A SOURCE OF PARTICULAR RISK OF MONEY LAUNDERING IN RELATIONS WITH THIRD COUNTRIES

Actions in the field of combating money laundering, carried out by international organisations and institutions, therefore, boil down primarily to the development of mechanisms to protect financial systems against this practice. For obvious reasons, cooperation based on standards developed on the international forum is desirable (and expected). The role of the global 'guarantor' in the field of preventing and combating money laundering is undoubtedly played by the Financial Action Task Force (FATF). On 28 October 2021, the FATF presented an updated *Risk-Based Approach Guide*.[65] The organisation draws attention to the need

---

[57] Ibidem, pp. 1–2.

[58] Cf. INTERPOL, *Online African Organized Crime…*, op. cit., pp. 20–32.

[59] Ibidem.

[60] On drug trafficking in the 'darknet', see Ocieczek, G., Opitek, P., 'Praktyczne aspekty zwalczania przestępczości narkotykowej dokonywanej w »świecie realnym« i cyberprzestrzeni', *Prokuratura i Prawo* 2022, No. 7–8, pp. 243–251. See also *Scams & Swindles…*, op. cit., pp. 133–148.

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

[62] On terminology: cf. Behan, A., *Waluty wirtualne jako przedmiot przestępstwa*, Kraków, 2022, pp. 237–242. Krasuski, K., Kharif, O., 'Crypto Capital Official Nabbed in Polish Money Laundering Probe', *Bloomberg News*, 25 October, 2019, https://www.bnnbloomberg.ca/crypto-capital-official-nabbed-in-polish-money-laundering-probe-1.1337624 [accessed on 10 January 2023].

[63] Proceedings with the participation of the Polish Prosecutor's Office – cf. e.g.: Krasuski, K., Kharif, O., *Crypto Capital Official…*, op. cit.

[64] Opitek, P., 'Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML', *Prokuratura i Prawo*, 2020, No. 12, p. 54.

[65] FATF, *Virtual Assets*, available at: https://www.fatf-gafi.org/en/topics/virtual-assets.html, and FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html [accessed on 26 February 2023].

for virtual asset service providers to apply the same financial security measures as applied to other obliged entities. Therefore, VASPs in particular should be subject to Customer Due Diligence (CDD), record keeping, transaction monitoring, and Reporting of Suspicious Transactions (STR). 'Under scrutiny' were, among others, cryptocurrency exchanges, cryptomat operators, crypto hedge funds, crypto wallet administrators and stablecoin administrators.[66] The updated recommendations also provide a recommendation on the licencing and registration of VASPs, as well as the additional recommendation for the public and private sectors on the implementation of the Travel Rule.[67] In the opinion of the FATF, the implementation of these guidelines determines efficient and effective cooperation in combating this form of *cyber-laundering,* while ensuring the transparency of transactions carried out using virtual assets.

From the perspective referred to in this study, the basic problem becomes the double criminality of crimes committed with the use of virtual assets. It is enough to point out the far-reaching differences in regulations. For example, in countries such as Algeria, Bolivia, Morocco, Nepal, Pakistan, or Vietnam, any activity related to cryptocurrencies is prohibited.[68] On the other hand, in others, such as Qatar and Bahrain, it is permissible for citizens of these countries, if the activity itself is carried out outside these countries. There are jurisdictions (e.g. Bangladesh, Iran, Thailand, Colombia, and China – from 2021) where only private transactions are allowed[69] or only a partial ban on cryptocurrency trading is in place (e.g. Iran allows cryptocurrency transactions from 2022 in imports[70]). Finally, we can point to legal solutions such as those in force since 2017 in the People's Republic of China, which prohibit *Initial Coin Offerings* (ICOs), i.e., obtaining cryptocurrencies or digital tokens through *crowdfunding,* similar to the first public offering (usually new) tokens.[71] More recently, in September 2021, the Chinese government also declared all private cryptocurrency transactions illegal, citing concerns about speculative investments, extreme price volatility, gambling scams, and money laundering.[72]

Upon discussing the risks of using cryptocurrencies for money laundering purposes, one should also remember those predicate acts that are (theoretically) 'traditional' crimes. It can be pointed out here, e.g., illegal entry, ransom extortion,

---

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

67 FATF Recommendation 16 imposes the obligation to identify the customer and beneficiary (VASP) and collect and store financial transactions using VA.

68 From: Riley, J., 'The Current Status of Cryptocurrency Regulation in China and Its Effect around the World', *China and WTO Review*, 2021, Vol. 7, No. 1, p. 139. http://dx.doi.org/10.14330/cwr.2021.7.1.06.

69 Riley, J., 'The Current Status of Cryptocurrency…', op. cit., p. 139.

70 www.iranintl.com/en/202208293261; on difficulties with transactions involving Bitcoin and the Iranian gold-backed digital currency PayMon: https://bitcoinpl.org/iranskia-waluta-cyfrowa-paymon [accessed on 27 February 2023]. On the topic of e-Gold and gold security – cf. Behan, A., *Waluty wirtualne…*, op. cit., pp. 40–46.

71 Ibidem, pp. 139–146, and also: Allen, F., Gu, X., Jagtiani, J., 'Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China', *Working Papers – Federal Reserve Bank of Philadelphia*, 2022, 22–12, p. 3. https://doi.org/10.21799/frbp.wp.2022.12.

72 Allen, F., Gu, X., Jagtiani, J., 'Fintech, Cryptocurrencies, and CBDC…', op. cit., p. 3.

theft, appropriation, etc., but committed using modern *blockchain technologies*[73] (or, for example, *the hash tree method* used by *Ripple* in XRP cryptocurrency transactions[74]). Examples of such crimes include hacking into electronic wallets, extorting ransom in cryptocurrencies, cryptojacking,[75] or appropriation of (often illegally obtained) bitcoins.[76] It should be noted that the very process of laundering, even when using virtual currency, often relies on methods of laundering known for years, i.e. *smurfing* and *structuring*.[77] Thus, transactions are typically based on accounts set up by 'mules', which are exchanged by them for cryptocurrencies, and then transferred to cryptocurrency wallets maintained by local virtual asset service operators. An example is a large-scale deal that took place in South Africa, discovered based on a suspicious transaction report submitted by a local VASP.[78] It involved the purchase of large amounts of virtual assets by various people and their immediate transfer to foreign VASPs. In many cases, different people had the same residential address and most addresses of these wallets were accessible from the same IP address. This led to the suspicion that they were being used as 'money laundering schemes'. To obscure the origin of illegal assets, cash transactions were carried out in the first stage, consisting of depositing funds in various accounts at various financial institutions. Then, they were transferred via electronic payments to other accounts to finally purchase cryptocurrency (bitcoins) in local VASPs. More than 150 people participated in this process, responsible for transferring a total of approximately 108,352,900 dollars (11,960 bitcoins).[79] Another example of

---

[73] *Blockchain* (*blockchain* technology) is a 'chain of blocks' that are used to store and transmit information about transactions concluded on the Internet. Its practical meaning lies in the possibility of one entity transferring to another 'a unique fragment of Internet property rights in a safe, open manner and on such terms that no one can question the legality of such a transaction' – cf. Zych, J., *Teleinformatyka dla bezpieczeństwa*, Poznań, 2019, pp. 133–134.

[74] Cf.: Kowalczyk, M., 'Ripple – czym jest i czy warto zainwestować?', *Cykl: kryptowaluty*, 11 October 2021, available at: https://www.najlepszekonto.pl/ripple-czem-jest-czy-inwestowac [accessed on 25 February 2023], and about the XRP digital currency: McDonalds, O., *Cryptocurrencies: Money, Trust and Regulation*, Newcastle, 2021, pp. 29–32.

[75] According to the definition of the Office of the Polish Financial Supervision Authority, *crypto-jacking* is: 'a type of cybercrime consisting in infecting and using, without the knowledge and consent of the user, the computing power of a device equipped with a processor (...) to mine cryptocurrencies': https://cebrf.knf.gov.pl/encyklopedia/hasla/385-definicje/797-cryptojacking. See also: Kropopek, K., '»Cryptojacking« wzrósł do rekordowego poziomu, pomimo załamania na rynku', *Comparic*, 28 July 2022, available at: https://comparic.pl/cryptojacking-wzrosl-do-rekordowego-level-despite-the-market-collapse/ [accessed on 26 February 2023], and: SonicWall, *2022 SonicWall Cyber Threat…*, op. cit., pp. 31–33.

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

[77] *Smurfing* is all about carrying out many financial operations (e.g. to fragment the value of assets) by many persons substituted for this purpose (so-called poles, mules), while *structuring*, considered a variation of the former, boils down to many recurring payments to a given account (also 'partial') – cf.: Golonka, A., *Prawnokarne zagadnienia przeciwdziałania…*, op. cit., pp. 31–33, and also: Jasiński, W., *Pranie brudnych pieniędzy*, Warszawa, 1998, pp. 69–70; Wójcik, J.W., *Pranie pieniędzy. Kryminologiczna i kryminalistyczna…*, op. cit., pp. 108–111 (referring to them as payment fragmentation techniques).

[78] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, p. 6: https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html [accessed on 18 February 2023].

[79] Ibidem.

laundering with VASP was the use of a crypto exchange in South Korea, through which approximately 400 million won[80] (more than 300,000 euros) were laundered from *phishing scams*. In this case, money (from *phishing*), i.e. fiat currency, was exchanged for three different types of cryptocurrencies, in multiple transactions, to end up in one foreign VASP wallet after the transfer.[81] A particular danger is seen in the participation of cryptocurrency exchanges in countries such as China (despite the country's relatively restrictive regulations on cryptocurrency trading)[82] or North Korea (*blacklisted* by the FATF), where cryptocurrencies were stolen in 2022 worth approximately 1.7 billion dollars according to estimates.[83] More specifically, experts say that North Korea is 'turning to stealing cryptocurrencies to fund its nuclear arsenal'.[84] Cryptocurrencies are laundered using so-called mixers, which, based on a method known as *blending*, mix cryptocurrencies from different users to lose track of the origin of these assets. There are also reports of brokers in China and non-fungible tokens (NFTs) being used for this purpose.[85]

The choice of the examples of money laundering using cryptocurrencies and the participation of VASPs located in China and North Korea in them was not accidental. These countries are relatively often indicated as a potential threat as regards their participation in the laundering of virtual currency. In relation to China and Hong Kong, it is said explicitly.[86] It is noted that: 'South American drug production and trafficking cartels use virtual currencies to launder money in China and Hong Kong. Bitcoin (…) aspires to be an international means of addressing the drug business.'[87] The threat is also seen by the American *Financial Crimes Enforcement Network* (FinCEN),[88] which recognised the Hong Kong-registered crypto exchange 'Bitzlato' (*Bitzlato Limited*) as 'a major money laundering concern'.[89] Bitzlato offered cryptocurrency exchanges and a vulnerable to money laundering *Peer-to-Peer* (P2P) service. The goal was to finance illegal Russian operations. This

---

[80] The South Korean Won (KRW) is the official currency of South Korea.

[81] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, p. 7, available at: https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html [accessed on 18 February 2023].

[82] *Initial Coin Offering* (ICO) is banned in China. On this issue and changes in the Chinese law regulating virtual assets trading – cf. Allen, F., Gu, X., Jagtiani, J., 'Fintech, Cryptocurrencies...', op. cit., s. 3.

[83] Ng, K., 'Crypto theft: North Korea-linked hackers stole $1.7b in 2022', *BBC News*, 2 February 2023. Article available at: https://www.bbc.com/news/world-asia-64494094 [accessed on 25 February 2023].

[84] Ibidem, and also: FinCEN, https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack [accessed on 25 February 2023].

[85] Ng, K., 'Crypto theft…', op. cit. Online article.

[86] Opitek, P., 'Przeciwdziałanie praniu…', op. cit., pp. 54–55.

[87] Ibidem, p. 54.

[88] https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering [accessed on 27 February 2023].

[89] The founder of Bitzlato is a Russian citizen, Anatoly Legkodymov (arrested by the US Department of Justice on 17 January 2023). Garcia, M., *Bitzlato Founder Charged With Facilitating Money Laundering of More than $700 Million in Dark Web Funds*, 3 February 2023, available at: https://www.whitecase.com/insight-alert/bitzlato-founder-charged-facilitating-money-laundering-more-700-million-dark-web [accessed on 25 February 2023].

was also possible due to the cooperation of *Hydra Market* – a Russian-speaking black market (i.e., operating on *the darknet*) and sanctions imposed on Russia after its invasion of Ukraine. *Darknet Hydra* shut down on 4 April 2022.[90] The sanctions also covered *Garantex*,[91] considered the most important platform used by cybercriminals for money laundering.[92]

From 1 January 2023, the United States has also implemented a regulation that officially bans Bitzlato transfers.[93] However, the fact remains that the sanctions and other restrictions imposed on trade with Russia have[94] not only failed to eliminate the risks associated with its possible involvement in laundering, but also revealed new cases of laundering of 'Russian money'. It is indicated that the state of South Dakota (USA) even aspires to be called a real world-class tax haven, due to the regulations in force there governing the establishment and operation of 'trusts'[95]. In fact, companies established in the form of trust funds make it possible for Russian oligarchs to invest money anonymously in them. It is even claimed that more than $350 billion is invested in trust funds in South Dakota and that the state legislature has been so completely taken over by the trust industry that there is no chance of changing the regulations.[96] In addition, a 'double standard' is apparent in the United States, as evidenced by the following practice: 'The US government demands information [on financial transactions – author's apposition] from other countries, while divulge details about foreigners' shares in its banks'.[97] This inconsistency hinders cooperation with the US in the field of anti-money laundering. Furthermore, there are indications of deficiencies in the applicable US regulations that dictate the

---

[90] Dr. Hack (*pseud.*), 'Największy na świecie rynek Darknet zamknięty', *SATKurier*, 6 April 2022, available at: https://satkurier.pl/news/216131/najwiekszy-na-swiecie-rynek-darknet-zamkniety.html [accessed on 25 February 2023].

[91] US Department of the Treasury, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, press release, 5 April, 2022, available at: https://home.treasury.gov/news/press-releases/jy0701 [accessed on 12 March 2023].

[92] 'Rosyjscy cyberprzestępcy szukają nowych sposobów prania pieniędzy. Wszystko przez wojnę', *CyberDefence24*, 25 April 2022, available at: https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjscy-cyberprzestepcy-szukaja-nowych-sposobow-prania-pieniedzy-wszystko-przez-wojne [accessed on 12 March 2023].

[93] Section 9714(a) of the *Combating Russian Money Laundering Act* (*Public Law* 116-283), as amended by S. 6106(b) *National Defense Authorization Act for Fiscal Year 2022* (*Public Law* 117-81).

[94] US Department of the Treasury, *Ukraine-/Russia-related Sanctions*, information available at: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions. Sanctions imposed by the EU: European Commission, *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 [accessed on 15 March 2023].

[95] Bullough, O., 'How Britain let Russia hide its dirty money', *The Guardian*, 25 May 2018, available at: https://www.theguardian.com/news/2018/may/25/how-britain-let-russia-hide-its-dirty-money [accessed on 15 March 2023].

[96] Boyce, J.K., Ndikumana, L., 'Kryzys w Ukrainie daje szansę na oczyszczenie brudnych pieniędzy', *Onet.pl*, 25 March 2022, available at: https://wiadomosci.onet.pl/politico/kryzys-na-ukrainie-gives-szanse-na-oczyczenia-brudnych-pieniedzy/zx0y3xf [accessed on 28 February 2023].

[97] Ibidem.

reporting suspicious transactions. Consequently, a situation arises where: 'a bank, after filing a suspicious activity report, can continue its business with the suspect customer. This is largely because most reports that are not publicly accessible are essentially ignored, akin to being covered in digital dust'.[98]

In turn, the British media write about financing Putin's war in Ukraine with values laundered in Great Britain,[99] which the British authorities do not even try to deny.[100] They only indicate the legislative steps they have taken or intend to take[101] (also in cooperation with other countries[102]) aimed at enforcing the sanctions imposed on Russia and counteracting money laundering. However, the fact remains that Russian oligarchs have been depositing huge sums of money in Great Britain for years (according to the British Office of National Statistics, Russian investments in this country were estimated at 25.5 billion pounds at the end of 2016[103]) and that 'dirty money' from Russia continues to contribute to the country budget. These funds used to be transferred from other countries, such as Cyprus, Bahamas, or financial havens (i.e., British Virgin Islands, Cayman Islands, Gibraltar, Jersey, and Guernsey). This made it possible to effectively hinder the detection of the country from which these funds actually came.[104] Currently, they are mainly transferred by countries that have not decided to include Russia in sanctions, such as Armenia, Vietnam, or China.[105]

Despite the ban on official economic contact with the Russian Federation introduced in many countries, resulting from the sanctions imposed on this country, many of them still maintain trade relations with Russia. Usually, this is not done

---

[98] Ibidem.

[99] Neate, R., 'UK failure to tackle »dirty money« led to it »laundering Russia's war funds«', *The Guardian*, 30 June 2022, available at: https://www.theguardian.com/business/2022/jun/30/uk-failure-to-tackle-dirty-money-led-to-it-laundering-russias-war-funds [accessed on 25 February 2023].

[100] Cf. House of Commons Foreign Affairs Committee, *The cost of compliance: 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, pp. 4, 6, available at: https://publications.parliament.uk/pa/cm5803/cmselect/cmfaff/688/report.html [accessed on 15 March 2023].

[101] House of Commons Committee Special Report, *The cost of complacency: illicit finance and the war in Ukraine: Government Response to the Committee's Second Report*, pp. 1–12, available at: https://publications.parliament.uk/pa/cm5803/cmselect/cmfaff/688/report.html [accessed on 15 March 2023].

[102] It is worth pointing out that since the withdrawal of the United Kingdom from the European Union under the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (OJ L 29, 31.1.2020, p. 7), the cooperation of this state with EU Member States in the field of criminal matters, regardless of the conventions to which the United Kingdom is a party, is regulated by the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, on the one hand, and the United Kingdom of Great Britain and Northern Ireland, on the other hand, from 31 December 2020. Cf. also: 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, No. 9, pp. 11–19.

[103] Bullough, O., *How Britain…*, op. cit.

[104] Ibidem.

[105] 'Rosyjscy cyberprzestępcy…', op. cit.

openly and legally, but through dealings with *offshore companies* 'with the cooperation of the best lawyers, auditors, bankers, and lobbyists in the world' who help Russian oligarchs develop legal ways to hide and launder their funds.[106] Such actions have been taking place for many years, even before Russia invaded Ukraine (also in European countries[107]). The current situation has only contributed to the perpetrators' search for new methods and ways to hide illegally obtained financial benefits.

JURISDICTION IN CYBERSPACE AND THE FIGHT AGAINST MONEY LAUNDERING

In addition to the difficulties related to the regulations concerning predicate acts, including the definition and regulation of cybercrimes, there are also specific issues related to the prosecution of these offences (both the predicate acts and money laundering) and the fact that they cover the territory of more than one country.[108] This, in turn, raises jurisdictional issues, most notably concerning crimes committed in cyberspace. This issue can be considered on three levels, i.e., legislative, executive, and judicial.[109] The term 'jurisdiction' is usually defined as 'the right of the state to encroach on the sphere of rights and duties of people' or 'the right of the state to regulate their behaviour in matters not only of an internal (national) nature'.[110] Jurisdiction is usually assumed to be territorial,[111] which is reflected in Polish criminal law by the principle of territoriality (Article 5 of the Polish Criminal Code). Derogations from it are provided for in Articles 109–113 of this Code (principles of international criminal law). However, as noted, the territorial application of the principle to 'this territorial creation that is cyberspace'[112] may prove problematic. This is due to the specific nature of such acts. Therefore, more than one proposal has been presented to resolve disputes regarding criminal jurisdiction in cases of crimes

---

[106] 'Russian oligarchs: Where do they hide their »dark money«?', *BBC News*, 28 March 2022, available at: https://www.bbc.com/news/world-60608282 [accessed on 15 March 2023].

[107] The routes of 'dirty' means led, among others, to Lithuania, Latvia, Estonia, Denmark, and Sweden, as well as Poland – cf. O'Donnell, J., 'Europol highlights Russian money as biggest laundering threat', *Reuters*, 14 June 2019, available at: https://www.reuters.com/article/us-europe-moneylaundering-europol-idUSKCN1TE2K6/; Harper, J., 'Russian money laundering comes to Poland', *Deutsche Welle*, 19 October 2020, available at: https://www.dw.com/en/how-ing-bank-in-poland-helped-russians-launder-money/a-55322399 [accessed on 15 March 2023].

[108] On this issue cf. Góral, K., Opitek, P., 'Analiza kryminalna transferów kryptowalutowych w pracy prokuratora', cz. II, *Prokuratura i Prawo*, 2020, No. 6, pp. 91–116.

[109] Czekalska, J., 'Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych', *Państwo i Prawo*, 2004, No. 11, p. 74.

[110] Beale, J.H., 'The Jurisdiction of a Sovereign State', *Harvard Law Review* (HLR), 1923, Vol. 36, p. 241, after: Płachta, M., 'Konflikty jurysdykcyjne w sprawach karnych: pojęcie, geneza i środki zaradcze', *Prokuratura i Prawo*, 2010, No. 11, p. 5.

[111] Mann, F.A., 'The Doctrine of Jurisdiction in International Law', *Recueil des Cours de l'Academie de droit international* (RCADI), 1964, Vol. 111, pp. 9–162, after: Płachta, M., 'Konflikty jurysdykcyjne…', op. cit., p. 75.

[112] Czekalska, J., 'Jurysdykcja w cyberprzestrzeni…', op. cit., p. 75.

in cyberspace.[113] It has even been postulated to consider cyberspace as the 'fourth space', as well as to introduce an exception from the principle of territoriality in favour of the principle of nationality.[114] Sharing the doubts about the difficulties caused by determining jurisdiction in cybercrime cases, it does not seem that the last of the proposed legal solutions is the best one (at least in the light of domestic criminal law, bearing in mind, however, a different approach to this issue in other criminal law systems).[115] It does not seem necessary to depart from the traditionally defined place of the act,[116] despite the undoubted specificity of crimes committed in cyberspace and the circumstances in which they occur (open architecture, independence from place, relative anonymity, etc., as features of cyberspace).[117] It remains obvious that the place of the act, in this case, may be both the place of the physical location of the host(s) and the server(s) (infrastructure), the actual presence of the perpetrator at the time of the act, and the place where the effect occurred (e.g. data theft). Thus, the jurisdiction of the state extends to perpetrators residing in its territory and to acts committed with the use of or against infrastructure located in its territory.[118] Judicial conflicts concerning such crimes should be resolved as in the case of all other multi-site crimes, i.e., based on criminal procedure procedures concerning international agreements accepted by a given state.[119] On the other hand, with regard to the legislative level and the principle of double criminality *in concreto*, one should be satisfied with the current method of determining the place(s) of the act(s). Otherwise, it would be more appropriate to consider establishing a separate rule, something like a 'cyber-territoriality' rule, which (perhaps) would lead to a consensus on determining one place of the act, but at the same time – highly likely – it would complicate the activities carried out in criminal proceedings in a cybercrime case. And there are quite a few of them. A significant amount of attention has been devoted to this subject, as evidenced by numerous publications.[120]

---

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

[114] In addition to Antarctica, outer space, and the open sea – Czekalska, J., 'Jurysdykcja w cyberprzestrzeni…', op. cit., pp. 74, 80–81.

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

[116] According to Art. 5 § 2 of the Penal Code, 'A prohibited act is deemed to have been committed in the place where the perpetrator acted or omitted to act to which he was obliged, or where the effect constituting the hallmark of the prohibited act occurred or was to occur according to the intention of the perpetrator.'

[117] Aleksandrowicz, T.R., 'Bezpieczeństwo w cyberprzestrzeni…', op. cit., p. 12.

[118] Ibidem, p. 24.

[119] Cf. Article 22 of the Council of Europe Convention on Cybercrime, drawn up in Budapest on 23 November 2001 (Journal of Laws of 2015, item 728), with a total of 67 signatories – see: https://pl.frwiki.wiki/wiki/Convention_sur_la_cybercriminalit%C3%A9 [accessed on 18 March 2023].

[120] Cf. e.g.: 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, No. 9, pp. 4–12; Kierzynka, R., 'Wzajemne uznawanie orzeczeń przepadku między państwami członkowskimi Unii Europejskiej', *Prokuratura i Prawo*, 2010, No. 9, pp. 16–21; Steinborn, S., 'Kolizje norm o międzynarodowej współpracy w sprawach karnych w zakresie zabezpieczenia mienia', *Europejski Przegląd Sądowy*, 2007, No. 4, pp. 15–25. Regarding the change of terminology and the replacement of

Additionally, explicit emphasis has been placed on the key challenges impeding the full and universal recognition and enforcement of foreign criminal judgments. These include state sovereignty, lack of equivalence of legal systems, lack of trust in international relations and difficulties resulting from the internal legal systems of individual countries.[121] Strategies to overcome these challenges have also been highlighted, such as obtaining agreement consent, employing the principle of reciprocity, engaging in the unification process, utilising the exequatur procedure, and applying the public policy clause.[122] Therefore, it is not surprising that the opinion expressed in the literature on the subject is that 'the principle of double criminality of an act often even prevents cooperation' and 'given the differences in legal regulations, the very definition of types of crime in acts of Community or EU law is difficult'.[123]

SMUGGLING OF MIGRANTS AND TRAFFICKING IN HUMAN BEINGS AND COMBATING MONEY LAUNDERING IN THE LIGHT OF FATF DOCUMENTS

When discussing the issue of international cooperation in combating money laundering and the related aspects connected with the current threats, it would be impossible not to mention one more, i.e., the smuggling of migrants. This problem is also recognised by the FATF.[124] As this organisation pointed out, migrant smuggling is inherently transnational and often involves moving people across borders for exploitation. Therefore, the threats of migrant smuggling and human trafficking, although they are different crimes,[125] cannot be completely separated. This also applies to the perspective of laundering the benefits derived from them. According to Frontex, the profits from such activities, subject to laundering, reach up to 10 billion dollars every year.[126] On the other hand, as regards human trafficking (as a predicate offence of money laundering), although it is certainly not a new phenomenon, the form and methods of committing this crime are subject to change.[127] Human trafficking, not only for sexual purposes but also in the form of, for example, organ trafficking, is increasingly taking place via the Internet. However, the preferred

---

the terms: 'requesting state' and 'requested state' with the terms: 'issuing state' and 'executing state' – Barwina, Z., *Zasada wzajemnego uznawania…*, op. cit., p. 157.

121 Aksamitowska-Kobos, M., 'Wnioski sądów polskich…', op. cit., p. 22.

122 Ibidem.

123 Hofmański, P., 'Przyszłość ścigania karnego w Europie', *Europejski Przegląd Sądowy*, 2006, No. 12, p. 5.

124 FATF, *Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling*, Paris, 2022, pp. 18–27, available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Migrant-smuggling.html [accessed on 15 February 2023].

125 Cf.: Jambor, J., 'Pokrzywdzony – ofiara handlu ludźmi w procedurach dochodzeniowych i sądowych', *Prokuratura i Prawo*, 2022, No. 9, p. 42.

126 FATF, *Money Laundering…*, op. cit., p. 18.

127 Mroczek, R., 'Formy inicjacji procesowej w sprawach o przestępstwa handlu ludźmi', *Prokuratura i Prawo*, 2019, No. 2, pp. 95–97.

form of payment is invariably cash (52%), followed by its transportation (literally) between jurisdictions.[128] For this purpose, the most popular methods include the use of *informal value transfer systems* (IVTS) such as *hawala* and recurring off-site prepaid card transactions.[129] This is rather significant from the perspective of counteracting money laundering and managing related criminal proceedings. The very issue of strategic activities and operational activities carried out in international cooperation in cases of human trafficking has been given enough space in the professional literature.[130] However, an analysis of the difficulties involved would go beyond the scope of this study. Taking into account the merits, and therefore the financial component of these offences, one should refer to the conclusions of the FATF report on the problem of migrant smuggling.[131] In the opinion of this organisation, the basic means of international cooperation in combating money laundering from such acts are: reliable collection, analysis, and exchange of financial information, as well as effective asset recovery.[132]

SUMMARY

To recapitulate, the issues presented above conclusively prove that money laundering as a practice is subject to constant change. They are conditioned both by the current global situation, particularly in the economic and political spheres, and by the development of modern technologies. The dynamics of socio-economic life, as well as the current political situation, create new opportunities for ingenious perpetrators of money laundering, while at the same time posing challenges to the authorities and institutions established to combat this practice.

Considering the fact that the crime of money laundering usually has a cross-border character and often extends beyond the territory of the European Union, it is important to take preventive actions against countries considered as posing a high risk as possible money laundering locations, and to develop rules of cooperation with countries outside the EU. It is evident that in addition to the need to develop legal regulations in this area, specific actions carried out in consultation with these countries are also necessary. Furthermore, one should not overlook the fact that, at the layering stage, money laundering is often committed in jurisdictions that, theoretically, do not raise concerns about the soundness of their financial systems. However, this does not mean that cooperation with these countries is devoid of problems. These are often rooted in the principle of double criminality, as evidenced by the difficulties arising from cryptocurrency transactions described in the study, as

---

[128] Yilmaz, A., *Money Laundering Rosks Arising from Migrant Smuggling*, 1 May 2022, https://dxcompliance.com/money-laundering-risks-arising-from-migrant-smuggling/ [accessed on 12 March 2023].

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

[130] See, for example: Galla-Podsiadło, K., Jakimko, W., Matyjewicz, M., Nowak, T., 'Współpraca międzynarodowa w sprawach o handel ludźmi', *Prokuratura i Prawo*, 2022, No. 9, pp. 170–229.

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

[132] Ibidem, pp. 34–35.

well as the consequences of the war in Ukraine in terms of commercial transactions. As indicated in the second part of the manuscript, cooperation with third countries may prove problematic both at the legislative and judicial levels. This is because third countries are not always willing to cooperate, alleging various formal or factual obstacles as reasons for non-cooperation. One such example include countries classified as tax havens. They make it difficult to trace the flow of 'dirty' asset values or prevent access to information on this subject. They also limit the effectiveness of actions taken by the bodies appointed to combat this phenomenon, in particular by the FIUs of other countries. It is undisputed that the transnational nature of the laundering process requires coordinated actions based on jointly developed legal measures.

On the international stage, not limited to EU countries, the FATF notably serves as the guardian of AML/CFT standards. Based on the documents developed by this organisation, as well as referring to the current threats in the field of money laundering, it should be recognised that the effectiveness of combating the practice requires strengthening bilateral and international cooperation both between the FIUs (including through the Egmont Group) and with law enforcement authorities and other authorities competent in the field of information exchange and mutual legal assistance. This applies in particular to countries that refer to national regulations, thus preventing the disclosure of essential circumstances of underlying acts or money laundering and the detection of their perpetrators. In addition to the necessity of abandoning barriers to the detection of principal crimes and their connection with the laundering of illegal financial benefits, it is also necessary to strengthen cooperation between neighbouring countries (border cooperation) to eliminate regional threats, mainly related to migration problems. Finally, recognising cybercrimes as a significant component of the predicate acts of money laundering, as well as cyber laundering as a form of its commission, it also seems indispensable to strive to develop coherent legal solutions in this area. These should include not only standards specifying the rules for collecting and transferring information about suspicious transactions, but also regulations enabling effective prosecution of their perpetrators and enforcement of adjudicated penalties.

BIBLIOGRAPHY

Aksamitowska-Kobos, M., 'Wnioski sądów polskich o wykonanie orzeczeń w sprawach karnych dotyczących kar o charakterze pieniężnym kierowane za granicę', *Iustitia*, 2015, No. 1.

Aleksandrowicz, T.R., 'Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego', *Przegląd Bezpieczeństwa Wewnętrznego*, 2016, Vol. 8, issue 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. 22-12.

Augustyniak, B., in: Świecki, D. (ed.), *Kodeks postępowania karnego. Tom II. Komentarz aktualizowany*, 6th ed., Warszawa, 2022.

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.

Boyce, J.K., Ndikumana, L., 'Kryzys w Ukrainie daje szansę na oczyszczenie brudnych pieniędzy', *Onet.pl*, 25 March 2022, available at: https://wiadomosci.onet.pl/politico/kryzys-na-ukrainie-gives-szanse-na-oczyczenia-brudnych-pieniedzy/zx0y3xf [accessed on 28 February 2023].

Brodowski, L., 'Zasada podwójnej karalności czynu w kontekście ekstradycji', *Studia Prawnicze KUL*, 2015, No. 1.

Bullough, O., 'How Britain let Russia hide its dirty money', *The Guardian*, 25 May 2018, available at: https://www.theguardian.com/news/2018/may/25/how-britain-let-russia-hide-its-dirty-money [accessed on 15 March 2023].

Czekalska, J., 'Jurysdykcja w cyberprzestrzeni a teoria przestrzeni międzynarodowych', *Państwo i Prawo*, 2004, No. 11.

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

Dr. Hack (*pseud.*), 'Największy na świecie rynek Darknet zamknięty', *SATKurier*, 6 April 2022, available at: https://satkurier.pl/news/216131/najwiekszy-na-swiecie-rynek-darknet-zamkniety.html [accessed on 25 February 2023].

European Commission, *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 [accessed on 15 March 2023].

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*, 20 October 2022, available at: https://www.eurojust.europa.eu/news/money-laundering-cases-registered-agency-doubled-last-6-years-according-eurojusts-new-report [accessed on 7 March 2023].

FATF, *Money Laundering and Terrorist Financing Risks Arising from Migrant Smuggling*, Paris, 2022, available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Migrant-smuggling.html [accessed on 15 February 2023].

FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html [accessed on 26 February 2023].

FATF, *Virtual Assets*, available at: https://www.fatf-gafi.org/en/topics/virtual-assets.html [accessed on 26 February 2023].

FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, available at: https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html [accessed on 18 February 2023].

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, No. 9.

Garcia, M., *Bitzlato Founder Charged With Facilitating Money Laundering of More than $700 Million in Dark Web Funds*, 3 February 2023, available at: https://www.whitecase.com/insight-alert/bitzlato-founder-charged-facilitating-money-laundering-more-700-million-dark-web [accessed on 25 February 2023].

Gardocki, L., 'Podwójna przestępność czynu w prawie ekstradycyjnym', in: *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', in: Łabuz, P., Malinowska, I., Michalski, M. (eds), *Przestępczość zorganizowana. Aspekty prawne kryminalno-kryminalistyczne*, Warszawa, 2022.

Góral, K., Opitek, P., 'Analiza kryminalna transferów kryptowalutowych w pracy prokuratora', part II, *Prokuratura i Prawo*, 2020, No. 6.

Grzelak, A., Kolowca, I., *Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości Unii Europejskiej. Współpraca policyjna i sądowa w sprawach karnych. Dokumenty*, Vol. 1, 1st ed., 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, No. 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', in: Grzywacz, J. (ed.), *Pranie brudnych pieniędzy*, Warszawa, 2005.

Harper, J., 'Russian money laundering comes to Poland', *Deutsche Welle*, 19 October 2020, available at: https://www.dw.com/en/how-ing-bank-in-poland-helped-russians-launder-money/a-55322399 [accessed on 15 March 2023].

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, No. 12.

House of Commons Committee Special Report, *The cost of complacency: illicit finance and the war in Ukraine: Government Response to the Committee's Second Report*, available at: https://publications.parliament.uk/pa/cm5803/cmselect/cmfaff/688/report.html [accessed on 15 March 2023].

House of Commons Foreign Affairs Committee, *The cost of compliance: illicit finance and the war in Ukraine. Second Report of Session 2022–23 Report, together with formal minutes relating to the report*, available at: https://publications.parliament.uk/pa/cm5803/cmselect/cmfaff/688/report.html [accessed on 15 March 2023].

IEWG, *FIU-FinTech Cooperation and Associated Cybercrime Typologies and Risks*, Ottawa, 2022.

INTERPOL, *Online African Organized Crime from Surface to Darkweb. Analytical report*, 2020.

Jambor, J., 'Pokrzywdzony – ofiara handlu ludźmi w procedurach dochodzeniowych i sądowych', *Prokuratura i Prawo*, 2022, No. 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, No. 9.

Kosiński, J., *Paradygmaty cyberprzestępczości*, Warszawa, 2015.

Kowalczyk, M., 'Ripple – czym jest i czy warto zainwestować?', *Cykl: kryplowaluty*, 11 October, 2021, https://moneteo.com/artykuly/ripple-czym-jest-czy-inwestowac [accessed on 23 November 2023].

Krasuski, K., Kharif, O., 'Crypto Capital Official Nabbed in Polish Money Laundering Probe', *Bloomberg News*, 25 October, 2019, https://www.bnnbloomberg.ca/crypto-capital-official-nabbed-in-polish-money-laundering-probe-1.1337624 [accessed on 10 January 2023].

Kropopek, K., '»Cryptojacking« wzrósł do rekordowego poziomu, pomimo załamania na rynku', *Comparic*, 28 July 2022, available at: https://comparic.pl/cryptojacking-wzrosl-do-rekordowego-level-despite-the-market-collapse/ [accessed on 26 February 2023].

Krysztofiuk, G., 'Perspektywy współpracy sądowej w sprawach karnych w Unii Europejskiej', *Prokuratura i Prawo*, 2015, No. 7–8.

Krysztofiuk, G., 'Zasada wzajemnego uznawania orzeczeń w sprawach karnych w Traktacie Lizbońskim', *Prokuratura i Prawo*, 2011, No. 7.

Kuczyńska, H., 'Glosa do postanowienia Sądu Najwyższego z dnia 22 listopada 2011 r., sygn. IV KK 267/11', *Prokuratura i Prawo*, 2013, No. 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, No. 6.

KWP w Białymstoku, 'Jak przestępcy wykorzystują pandemię', *Policja997*, 2020, No. 182.

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, No. 7–8.

Marek, A., 'Komentarz do Konwencji w sprawie prania dochodów pochodzących z przestępstwa, ich ujawniania, zajmowania i konfiskaty', in: Zielińska, E. (ed.), *Standardy prawne Rady Europy. Teksty i komentarz. Tom III – Prawo karne*, Warszawa, 1997.

Maroń, H., 'Współpraca policyjna i sądowa w sprawach karnych wg projektu Konstytucji Europejskiej', *Państwo i Prawo*, 2007, No. 4.

McDonalds, O., *Cryptocurrencies: Money, Trust and Regulation*, Agenda Publishing, Newcastle, 2021 [ISBN: 978-1-78821-420-9].

Michalczuk, C., 'Współpraca prawna w sprawach karnych z »rajami podatkowymi«', *Prokuratura i Prawo*, 2010, No. 9.

Mika, J.F., Mika, M., 'Istota rajów podatkowych', in: Mika, J.F. (ed.), *Raje podatkowe. Procedura należytej staranności, obowiązki w cenach transferowych*, Warszawa, 2023.

Mroczek, R., 'Formy inicjacji procesowej w sprawach o przestępstwa handlu ludźmi', *Prokuratura i Prawo*, 2019, No. 2.

Neate, R., 'UK failure to tackle »dirty money« led to it »laundering Russia's war funds«', *The Guardian*, 30 June 2022, available at: https://www.theguardian.com/business/2022/jun/30/uk-failure-to-tackle-dirty-money-led-to-it-laundering-russias-war-funds [accessed on 25 February 2023].

Ng, K., 'Crypto theft: North Korea-linked hackers stole $1.7b in 2022', *BBC News*, 2 February 2023, available at: https://www.bbc.com/news/world-asia-64494094 [accessed on 25 February 2023].

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, No. 9.

Obczyński, R., in: Kapica, W. (ed.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa, 2020.

Ocieczek, G., Opitek, P., 'Praktyczne aspekty zwalczania przestępczości narkotykowej dokonywanej w »świecie realnym« i cyberprzestrzeni', *Prokuratura i Prawo*, 2022, No. 7–8.

O'Donnell, J., 'Europol highlights Russian money as biggest laundering threat', *Reuters*, 14 June 2019, available at: https://www.reuters.com/article/us-europe-moneylaundering-europol-idUSKCN1TE2K6/ [accessed on 15 March 2023].

Opitek, P., 'Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML', *Prokuratura i Prawo*, 2020, No. 12.

Płachta, M., 'Konflikty jurysdykcyjne w sprawach karnych: pojęcie, geneza i środki zaradcze', *Prokuratura i Prawo*, 2010, No. 11.

Płachta, M., 'Uznawanie i wykonywanie zagranicznych orzeczeń karnych. Zagadnienia podstawowe', *Państwo i Prawo*, 1985, No. 3.

Pszczółkowski, S., *Zagadnienie podwójnego opodatkowania w stosunkach międzynarodowych*, (doctoral dissertation accepted by the UW Law Faculty Board by resolution of 1 May 1925), 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, No. 1.

Rojszczak, M., 'Cyberbezpieczeństwo 2.0: w poszukiwaniu nowych ram ochrony cyberprzestrzeni', in: Banasiński, C., Rojszczak, M. (eds), *Cyberbezpieczeństwo*, Warszawa, 2020.

'Rosyjscy cyberprzestępcy szukają nowych sposobów prania pieniędzy. Wszystko przez wojnę', *CyberDefence24*, 25 April 2022, available at: https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjscy-cyberprzestepcy-szukaja-nowych-sposobow-prania-pieniedzy-wszystko-przed-wojne [accessed on 12 March 2023].

'Russian oligarchs: Where do they hide their »dark money«?', *BBC News*, 28 March 2022, available at: https://www.bbc.com/news/world-60608282 [accessed on 15 March 2023].

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, 1st ed., Los Angeles, 2006. [ISBN: 978-1-56343-786-1, 978-1-280-91928-2].

SonicWall, *2022 SonicWall Cyber Threat Report*, available at: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf. [accessed on 24 November 2023].

Steinborn, S., in: Grzelak, A., Królikowski, M., Sakowicz, A. (eds), *Europejskie prawo karne*, 1st ed., Warszawa, 2012.

Steinborn, S., 'Kolizje norm o międzynarodowej współpracy w sprawach karnych w zakresie zabezpieczenia mienia', *Europejski Przegląd Sądowy*, 2007, No. 4.

Szumski, A., 'Współpraca międzynarodowa w zwalczaniu przestępczości zorganizowanej na obszarach dawnych konfliktów etnicznych na przykładzie misji EULEX Kosowo', *Wschodnioznawstwo*, 2016, No. 10.

Szwarc, A.J., Długosz, J., 'Unijne instrumenty współdziałania państw w sprawach karnych', *Edukacja Prawnicza*, 2011, No. 3.

US Department of the Treasury, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, 5 April 2022, available at: https://home.treasury.gov/news/press-releases/jy0701 [accessed on 12 March 2023].

US Department of the Treasury, *Ukraine-/Russia-related Sanctions*, available at: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions [accessed on 15 March 2023].

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

Weerth, C., 'INTERPOL on COVID-19: Urgent Safety alert – Results of the 2020 fake medicine and medicine products operation PANGEA XIII', *Technical Report*, March 2020.

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

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

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

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

Yilmaz, A., *Money Laundering Rosks Arising from Migrant Smuggling*, 1 May 2022, https://dxcompliance.com/money-laundering-risks-arising-from-migrant-smuggling/ [accessed on 12 March 2023].

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

Zaród, M., 'Hakerzy i kolektywy hakerskie w Polsce. Od operacjonalizacji do laboratoriów i stref wymiany', *Studia Socjologiczne*, 2017, Vol. 1, No. 224.

Zych, J., *Teleinformatyka dla bezpieczeństwa*, 2nd ed., Poznań, 2019.

Cite as:

Golonka A. (2023) *'Cooperation with third countries in combating money laundering in the face of modern challenges'*, Ius Novum (Vol. 17) 4, 15–39. DOI 10.2478/in-2023-0027