Łukasz Krupa*

Money laundering and cybercrime

Abstract

In order to be used legally, proceeds from criminal activity must be laundered first. One type of crime that can be linked to money laundering is cybercrime, which has to be fought with special tools allowing for operation in cyberspace. Money laundering, and the related financing of terrorism and organised crime, pose a major threat to state security and financial stability.

Key words: cyberspace, cybercrime, money laundering

* Łukasz Krupa, Kancelaria Krupa i Partnerzy Adwokaci i Radcowie Prawni, e-mail: l.krupa@kiplegal.com.

Money laundering is a follow-up crime to an underlying one. This means that one cannot speak of money laundering unless another criminal act has been committed prior to it. The reason is that if the funds come from a legitimate source and have been earned, for example by working, running a business, receiving an inheritance, etc., then they cannot be subjected to a „laundering" process. Therefore, it is assumed that, in order to determine that a money laundering crime has been committed, an „underlying crime" must occur first. At this point, it should be noted that there is a discrepancy between money laundering law and compliance doctrine. The latter refers to the underlying crime from which the funds originate. In turn, pursuant to Art. 299 of the Code of Criminal Procedure, money laundering occurs if the funds originate from a prohibited act. The concept of a prohibited act is much broader and also includes minor offences. It is important to correctly establish what the underlying act consisted of, as well as what benefits it generated so that only the actions undertaken concerning these benefits can be analysed in terms of the features of a criminal offence. There is no doubt that money laundering is a derivative act with regard to the underlying act[1] Money laundering is, therefore, a follow-up act to the underlying offence[2].

Pursuant to Art. 299 of the Criminal Code, anyone who receives, possesses, uses, conveys or transports abroad, conceals, transfers or converts legal tenders, financial instruments, securities, foreign exchange, property rights or other movable or immovable property, which are connected to any criminal offence, or undertakes other actions that may frustrate or significantly hinder the determination of their criminal origin or location, their detection, seizure or forfeiture, shall be liable to imprisonment for a term between six months to ten years. This sanction also applies to an employee or anyone acting in the name of, or for the benefit of, a bank, financial or credit institution, or another entity legally, which is required by law to register transactions and who receives legal tenders, financial instruments, securities, foreign exchange, transfers or converts them or receives them in circumstances raising a reasonable suspicion that they are the object of the act referred to in this provision or provides other services aimed at concealing their criminal origin or securing them from seizure. If the perpetrator commits these acts in collaboration

1 Judgement of the Court of Appeal in Szczecin of 24 June 2021, II AKa 248/20, LEX no. 3228435.

2 Ł. Krupa, *Przeciwdziałanie finansowaniu terroryzmu*, „Cybersecurity and Law" 2022, no. 1, p. 98.

with other persons, he or she shall be punished by imprisonment for a term of one to ten years. In the event of passing judgement convicting an individual of the offence of money laundering, the court orders the forfeiture of objects originating directly or indirectly from the offence, as well as the proceeds of the offence or the equivalent thereof, even if they are not the property of the offender. Forfeiture, in whole or in part, is not ordered if the object, benefit or the equivalent thereof is to be returned to the victim or another entity. An individual who has voluntarily disclosed to a law enforcement authority information concerning persons participating in an offence and the circumstances thereof is not subject to punishment for the offence of money laundering if this has helped to prevent another offence. If the offender has made efforts to disclose such information and circumstances, the court applies extraordinary mitigation of punishment.

To satisfy the criteria of the legal definition of the offence of money laundering, no special conditions are required. The procedure is conducted in stages. The first stage involves the transfer of illicit funds from criminal activity into a venture based on capital with a legitimate source. Such a combination is intended to give the appearance of the legitimacy of the source of funds originating from criminal activity and to introduce them as legitimate capital into the financial system. However, the view that in order to fulfil the criteria of the analysed offence, the fulfilment of all stages is required, leading to the „laundering" of the deposited funds, is not legitimate. Criminalisation covers each of the stages of the procedure, including the very act of depositing (investing) such funds[3].

The European Union, by way of a Directive[4], introduced minimum criteria for the definition of offences and penalties in the area of money laundering, expressly providing that money laundering, and the related financing of terrorism and organised crime, continue to be a serious problem at the level of the European Union, damaging the integrity and stability of the financial sector and endangering both the internal market and the internal security of the European Union. Pursuant to Art. 2(1) of this Directive, criminal activity related to money laundering is defined as any criminal involvement in an

3 Judgement of the Court of Appeal in Warsaw of 17 November 2017, II AKa 289/17, LEX no. 2412810.

4 Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by means of criminal law (Official Journal of the European Union 2018, L 284/22).

offence punishable by imprisonment or a detention order for more than one year under domestic law or, in the case of the Member States whose legal systems provide for a minimum threshold for offences, offences punishable by imprisonment or a detention order for a minimum of six months. This also includes cybercrime.

EU legislation points out that, in order to effectively combat cybercrime, it is necessary to increase the resilience of information systems by making them more secure against cyber-attacks, which requires the adoption of appropriate measures. Member States should take appropriate measures to adequately protect critical infrastructure from cyber-attacks. An adequate level of protection against reasonably identifiable threats and vulnerabilities should be provided under the state of technology in each sector and the specific requirements of data processing. The costs of such protection should be proportionate to the likely damage that a potential cyber-attack could cause. Member States are required to take any necessary measures to ensure that: 1) intentional and unlawful access to all or any part of an information system is punishable as a criminal offence when committed in breach of security measures, at least in cases which are not deemed as minor (unlawful access to information systems); 2) intentional and unlawful serious obstruction or interference with the functioning of an information system by introducing, transmitting, damaging, deleting, deteriorating, altering or eliminating computer data or rendering it inaccessible is punishable as a criminal offence, at least in cases that are not deemed as minor (unlawful interference with systems); 3) intentional and unlawful deletion, damaging, deteriorating, altering or eliminating computer data in an information system or rendering it inaccessible is punishable as a criminal offence, at least in cases that are not deemed as minor (unlawful interference with data); 4) intentional and unlawful interception by technical means of non-public transmission of computer data to, from or within an information system, including electromagnetic emissions from an information system containing such computer data, is punishable as a criminal offence, at least in cases that are not deemed as minor (unlawful interception)[5].

The threats posed by underlying crimes are described in detail in the National Risk Assessment. As noted, underlying crimes to money laundering

5 Directive 2013/40/UE of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Official Journal of the European Union 2013, L 218/8).

can be considered as any type of offence, whereby the offender obtains assets. Underlying crimes may include corruption, offences on the financial market (including stock market offences, insurance-related offences, operating without licences, etc.), tax offences, illicit trafficking in narcotic drugs and psychotropic substances, human trafficking and the smuggling of migrants, illegal gambling, offences related to the infringement of copyright and industrial property rights, offences against property and economic turnover, as well as other offences[6].

It has to be pointed out that counteracting money laundering has a significant impact on state security, not only in terms of preventing the act itself but also in terms of limiting the proceeds from such criminal acts. Thus, the effective prevention of money laundering can translate into reducing the profitability of committing other crimes.

Cybercrime, including offences related to money laundering, compromises cybersecurity which is defined as the resilience of information systems to measures that compromise the confidentiality, integrity, availability and authenticity of the data processed or the related services offered by those systems[7]. Given the above, special attention should be paid to ensuring protection against and combating such crimes, especially given the fact that the use of cyberspace is widespread, including for such purposes as implementing tasks of fundamental importance for the state and its security[8].

6 *Krajowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu*, https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu [dostęp: 20.08.2022].

7 Art. 2(4) of the Act of 5 July 2018 on the national cybersecurity system (consolidated text, Journal of Laws 2022, item 1863). On the issue of cybersecurity, see also: M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; M. Karpiuk, *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, no. 2; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; M. Karpiuk, *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

8 On the issue of security, see also: M. Czuryk, *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, no. 3; M. Karpiuk, *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, no. 2; M. Czuryk, *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017; K. Chałubińska-Jentkiewicz, M. Karpiuk, K. Zalasińska, *Prawo bezpieczeństwa kulturowego*, Siedlce 2016; M. Karpiuk, *Position of County Government in the Security Space*, „Internal

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.
Chałubińska-Jentkiewicz K., Karpiuk M., Zalasińska K., *Prawo bezpieczeństwa kulturowego*, Siedlce 2016.
Czuryk M., *Bezpieczeństwo jako dobro wspólne*, „Zeszyty Naukowe KUL" 2018, no. 3.
Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.
Czuryk M., *Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny*, „Roczniki Nauk Społecznych" 2013, no. 3.
Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.
Czuryk M., *Właściwość Rady Ministrów oraz Prezesa Rady Ministrów w zakresie obronności, bezpieczeństwa i porządku publicznego*, Olsztyn 2017.
Karpiuk M., *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Position of County Government in the Security Space*, „Internal Security" 2019, no. 1.
Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, no. 2.
Karpiuk M., *Ubezpieczenie społeczne rolników jako element bezpieczeństwa społecznego. Aspekty prawne*, „Międzynarodowe Studia Społeczno-Humanistyczne. Humanum" 2018, no. 2.
Karpiuk M., *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, no. 2.
Krupa Ł., *Przeciwdziałanie finansowaniu terroryzmu*, „Cybersecurity and Law" 2022, no. 1.

Pranie pieniędzy a cyberprzestępczość

Streszczenie

Działalność przestępcza jest źródłem dochodu, który musi być zalegalizowany, zatem pieniądze z tej działalności muszą być wyprane. Jednym z rodzajów przestępstw, które może być powiązane z praniem pieniędzy są cyberprzestępstwa. Ich zwalczanie wymaga szczególnych narzędzi pozwalających na działanie w cyberprzestrzeni. Pranie pieniędzy i związane z tym przestępstwem finansowanie terroryzmu, a także powiązana z tymi zjawiskami przestępczość zorganizowana stanowią duże zagrożenie dla bezpieczeństwa państwa i stabilności finansowej.

Słowa kluczowe: cyberprzestrzeń, cyberprzestępczość, pranie pieniędzy

Security" 2019, no. 1; M. Czuryk, *Podstawy prawne bezpieczeństwa narodowego w stanie kryzysu i wojny*, „Roczniki Nauk Społecznych" 2013, no. 3; M. Karpiuk, *Właściwość wojewody w zakresie zapewnienia bezpieczeństwa i porządku publicznego oraz zapobiegania zagrożeniu życia i zdrowia*, „Zeszyty Naukowe KUL" 2018, no. 2.