DR. JUDIT JACSÓ, FULL PROFESSOR

University of Miskolc / Vienna University of Economics and Business | DOI: 10.32041/9788367149761/4

Chapter 4. Preventive Means Against Cyber-Laundering in the European Union

4.1. Introduction

The dynamic change in money laundering methods requires regulatory authorities including those in the European Union (EU) to constantly modify their regulations to effectively combat these illicit activities. The chapter deals with the preventive measures of the European Union against money laundering, with regard to cyber-laundering. It is difficult to estimate the scale of money laundering, given the high latency rate for legalised amounts.[1] The same can be established with regard to cyber-laundering.[2] In accordance with the Europol-report, between 0.7–1.28% of annual EU GDP is identified as being involved in suspect financial activity.[3]

[1] The estimated amount of money laundered globally in one year is 2–5%. According to the study of Bussmann and Vockrodt, this amount could be over EUR 100 billion a year in Germany (K.D. Bussmann, M. Vockrodt, *Geldwäsche-Compliance im Nicht-Finanzsektor: Ergebnisse aus einer Dunkelfeldstudie*, "Compliance Berater" 2016, No. 5, p. 139).

[2] D.A. Leslie, *Legal Principles for Combatting Cyberlaundering*, New York 2014, pp. 4–5.

[3] Europol Financial Intelligence Group, *From suspicion to action converting financial intelligence into greater operational impact 2017*, p. 5, https://www.europol.europa.eu/publications-events/publications/suspicion-to-action-converting-financial-intelligence-greater-operational-impact#downloads (accessed on: 06.06.2023).

Since 1991, the European Union has been trying to create an effective and coherent framework against money laundering, which includes five anti-money laundering directives, requiring Member States to prescribe service providers with many obligations, the most important of which are the identification of their customers (Know Your Customer (KYC) and the Suspicious Transaction Reports (STRs)).

It is important to emphasise that the European Union regulation has been taken into account the international standards, especially the Forty Recommendations of the Financial Action Task Force (FATF) and international conventions of the United Nations and the Council of Europe[4] when formulating the obligations from the beginning. Several reports of international organisations and scientific studies pointed to the danger that the Anti-Money Laundering (AML) regime, which was created against the traditional forms of money laundering, was not adequate against money laundering using virtual methods, which in turn made it necessary to modify them and extend their scope to virtual assets (VAs) and virtual assets providers (VASPs).[5] At the 4th Global Conference on Cryptocurrencies and Criminal Finances conference held in November 2020, it was stated that VASPs should be regulated in the same way as other financial services and should also contribute to the fight against global money laundering.[6] An important and necessary first step in the action against virtual assets (cryptocurrency) laundering was the creation of a regulatory framework.[7]

---

[4] See the chapter about "New developments and challenges of the fight against money laundering by the cybercrime – methods and risks".

[5] Z. Céman, M. Hegedűs, *Pénzmosás mint negatív gazdasági tényező az Európai Unióban*, "Belügyi Szemle" 2023, No. 5, p. 885.

[6] See the 5 Recommendation of the Conference which was organised by Interpol, Basel Institute of Governance and Europol, https://baselgovernance.org/sites/default/files/2020-11/Crypto%20Conference%202020%20Recommendations.pdf (accessed on: 05.06.2023).

[7] See Ch. Rückert, *Phänomenologie,* [in:] Ph. Mauma, L. Maute, M. Fromberger, *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, München 2020, pp. 527–536; B. Brandl, J. Bülte, *Kryptowährungen/-assets – Geldwäsche und Terrorismusbekämpfung – Perspektive Sorgfaltsverpflichtete*, [in:] R. Leitner, R. Brandl (eds.), *Finanzstrafrecht 2022 Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, Vienna 2023, pp. 105–122.

In the first part of the study, we briefly summarise the development at international level with particular regard to the FATF Recommendations, according to which the European Union preventive regulations have also constantly been changed. Among the wide range of preventive instruments against money laundering (cyber laundering), the focus is on the risk-based approach, which is fundamentally of a basic nature, the reporting obligation and the role of the Financial Intelligence Unit (FIU). After this, the latest developments in the EU will be examined and the resulting proposals will also be covered. When outlining development trends, the focus is on the examination of the effectiveness of action against new forms of money laundering, with particular attention to VAs and VASPs.

4.2. Global Standard (FATF Recommendations) in Connection to VAs and VASPs

4.2.1. REGULATORY DEVELOPMENT

The FATF's 40 Recommendations[8] were first published in 1990. FATF has modified and revised the recommendations several times. The FATF Recommendation provides countries with a comprehensive framework to combat illicit financial flows. The document contains the following 7 parts:

1. AML/CFT policies and coordination,
2. money laundering and confiscation,
3. terrorist financing and the financing of proliferation,
4. preventive measures,
5. transparency and beneficial ownership of legal persons and arrangements,
6. power and responsibilities of competent authorities and other institutional measures,
7. international cooperation.

[8] The FATF Recommendations International Standards on Combating Money Laundering and Terrorism & Proliferation, updated February 2023. See: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (accessed on: 3.06.2023).

It should be highlighted that the Recommendations use the risk--based approach (RBA), which means:

> countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively.[9]

Countries must distinguish between high and low risk and adapt the necessary measures accordingly. This basic concept encourages a more efficient allocation of resources.

The FATF recognised that new and innovative payment products and services are developed which have the potential of being used for money laundering or terrorist financing.[10] The FATF has developed guidance for countries and the private sector on how to apply a risk-based approach to implementing AML/CFT measures. With the development of digitalisation, the risk of money laundering increased. Recognising this, the New Payment Products and Services Guidance[11] was published as a first step in 2013. This guidance examines how these payment products and services work, and how to regulate and supervise this activity. It deals with the risks of prepaid cards, mobile payments and internet-based payment. However, the FATF Guidance was not addressed to virtual currencies. It only notes that whereas "some alternative currencies, such as decentralised digital currencies, may fall outside the scope of this guidance, the guidance remains relevant where such currencies are exchanged or redeemed."[12]

---

[9] See FATF Recommendation 1.

[10] See J. Grzywot, *Virtuelle Kryptowährungen und Geldwäsche*, Internetrecht und Digitale Gesellschaft, Band 15, Berlin 2019, p. 90.

[11] Guidance for a risk-based approach – prepaid-cards, mobile payments and internet-based payment services, June 2013, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-npps-2013.html (accessed on: 03.07.2023).

[12] Guidance for a risk-based approach – prepaid-cards, mobile payments and internet-based payment services, June 2013, p. 3.

Recognising that virtual currencies would spread in the coming years, and that national policy responses vary considerably, the FATF issued a first report about virtual currencies in 2014.[13] The importance of the report is further enhanced by the fact that it examines the risks associated with crypto-currencies, provides a common definitional vocabulary (virtual currency, digital currency) and classifies the types of virtual currency (convertible/open and non-convertible/closed virtual currency, centralised and non-centralised virtual currency, etc.).[14]

The next step was in June 2015, with the establishment of the "Guidance for a Risk-Based Approach to Virtual Currencies"[15] In October 2018, the FATF Plenary discussed and adopted amendments to the FATF Standards to respond to the increasing use of virtual assets for money laundering and terrorist financing. In 2019, FATF extended the AML/CFT measures to VAs and VASPs to prevent criminal and terrorist misuse of the sector. In 2019, the "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (VASPs)" was adopted, in order to help the national authorities, supervisory, private sector entities understand their AML/CFT actions and obligations. The VASPs have the same obligations as financial institution (especially KYC).[16] The money laundering offence should extend:

[13] FATF Report Virtual Currencies – Key Definitions and Potential Anti-money Laundering and Counter-terrorist Financing Risks, June 2014, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html (accessed on: 02.08.2023).

[14] See more about the definition in the chapter "New developments and challenges of the fight against money laundering by the cybercrime – methods and risks".

[15] FATF Guidance for a risk-based approach Virtual currencies, June 2015, https://www.fatf-gafi.org/en/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html (accessed on: 06.06.2023).

[16] R. Brandl, J. Bülte, *Kryptowährungen/-assets – Geldwäsche und Terrorismusbekämpfung – Perspektive Sorgfaltsverpflichtete*, [in:] R. Leitner, R. Brandl (eds.), *Finanzstrafrecht 2022 Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, Linde Verlag, Vienna 2023, pp. 113–114.

> to any type of property, regardless of its value, that directly represents the proceeds of crime, including in the context of VAs. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence, including in the case of VA-related proceeds. Countries should therefore extend their applicable ML offence measures to proceeds of crime involving VAs.

The same comprehensive approach is applied by the confiscation and provisional measures.

In July 2021, the FATF adopted the report "Opportunities and Challenges of New Technologies for AML/CFT".[17] In October 2021, the "Guidance for a Risk-Based Approach – Virtual Assets and Virtual Asset Providers" was updated. In June 2023, the "Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs" was adopted.[18] Based on this, we present the following relevant recommendations.

4.2.2. FATF RECOMMENDATION NO. 15 AND FATF RECOMMENDATION NO. 16 (TRAVEL RULE)

The Recommendation No. 15 (Jurisdictions' Implementation of FATF Standards on VAs/VASPs) recognise the dangers associated with new technologies and states that:

> countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including

[17] FATF Opportunities and Challenges of new technologies for AML/CFT, July 2021, https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html (accessed on: 06.06.2023).

[18] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html (accessed on: 03.08.2023).

> new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products.

They should take appropriate measures to manage and mitigate those risks in order:

> to manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.[19]

The so-called "travel rule" is one of the key AML/CFT measures to combat cyber-laundering. In accordance with the wire transfer requirements, "Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain."[20] The travel rule applies in the VA context. The travel rule requires VASPs and financial institutions to obtain, hold, and transmit specific originator and beneficiary information immediately and securely when transferring VAs. Law enforcement authorities regard the travel rule as very important for the detection, investigation and prosecution of tmoney laundering, and helpful for financial intelligence units to analyse reports of suspected money laundering.[21]

In accordance with the latest report of the FATF in June 2023, the global implementation of Recommendation No. 15 is relatively poor; 75% of jurisdictions assessed against the revised standards are only partially or non-compliant with FATF's requirements

[19] FATF Recommendation No. 15

[20] FATF Recommendation No. 16

[21] FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, Paris 2023, p. 16, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html (accessed on: 03.08.2023).

in this matter.[22] However, the European Union legislator took an important step to protect this sector, and a regulatory framework for VASPs and the travel rule was established.

In summary, it can be concluded that the FATF has responded to the challenges posed by new technologies with phased approach. We can see that it took decisive steps against cyber-laundering with the framework of the preventive measures and laid down global standards in this area as well. In the next point we will research development and regulatory framework of the European Union, which is in line with the FATF's expectations.

4.3. Development of the AML Regulation in the European Union

Money laundering is a major threat to the global financial system and to economies generally, but it is a significant problem at the EU level too, because it damages the integrity, stability and reputation of the financial sector and the internal market and the internal security of the Union.[23] The legislator of the European Union is strongly committed to the fight against money laundering and terrorist financing.

4.3.1. MAIN CHARACTERISTICS OF THE AML REGULATION FRAMEWORK IN THE EU

The most important EU legal acts in connection with the money laundering are found in directive-level rules, which the member states must implement into their own national legal systems. The European Union's anti-money laundering policy can be said to

[22] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets.html (accessed on: 06.06.2023); FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, Paris 2023, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html (accessed on: 03.08.2023).

[23] Preamble 8 Art. 1 Directive (EU) 2015/849.

be based on two pillars: non-criminal (preventive/administrative) and criminal measures. Measures relating to money laundering compliance can essentially be included among the preventive instruments. The initial sectoral regulation, which imposed obligations only on financial and credit institutions, has now been replaced by a comprehensive concept that entails obligations for almost all economic operators.

There are five AML Directives which regulate the preventive instruments against money laundering:

- Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering[24] (I. AML Directive);
- Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering – Commission Declaration[25] (II. AML Directive);
- Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing[26] (III. AML Directive);
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC[27] (IV. AML Directive);
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system

[24] OJ EU L 166, 28.6.1991, pp. 77–82.
[25] OJ EU L 344, 28.12.2001, pp. 76–82.
[26] OJ EU L 309, 25.11.2005, pp. 15–36.
[27] OJ EU L 141, 5.6.2015, pp. 73–117.

> for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU[28] (V. AML Directive).

Their primary objective is to prevent the financial sector from being used for purposes of money laundering by requiring customer due diligence obligation and reporting obligation.[29] It is important to underline that the EU legislator took into account the FATF's Recommendations for all directives.

In addition, it is also necessary to mention the "Regulation on Transfers of Funds"[30] which serves to comply with the mentioned above FATF Recommendations No. 16. The regulation establishes requirements for financial institutions (banks, payment service providers, e-money issuers, etc.) to include specific information along with electronic money transfers or wire transfers, in order to help prevent, detect and investigate money laundering and terrorist financing.

In line with the FATF's Recommendation, the European Union's regulation uses a risk-based approach, which is implemented on the basis of multi-level regulations. This approach was described by the III. AML Directive, based on the provision of:

> Member States require that institutions and persons covered by this policy shall establish appropriate policies and procedures for customer due diligence, reporting, registration, internal control, risk assessment, risk management,

---

[28] OJ EU L 156, 19.6.2018, pp. 43–74.

[29] See in detail: B. Udvarhelyi, *Pénzmosás elleni küzdelem az Európai Unióban.* [in:] I. Stipta (ed.), *Studia Iurisprudentiae Doctorandorum Miskolciensium – Miskolci Doktoranduszok Jogtudományi Tanulmányai*, Tomus 12., Miskolc 2013, pp. 456–464, 467–469; A. Met-Domestici, *The Reform of the Fight against Money Laundering in the EU*, "Eucrim" 2013, No. 3, pp. 170–179; D. Langlois, *The Revision of the EU Framework on the Prevention of Money Laundering*, "Eucrim" 2013, No. 3, pp. 96–98; A. Met-Domestici, *The Fight against Money Laundering in the EU – The Framework Set by the Fourth Directive and its Proposed Enhancements*, "Eucrim" 2016, No. 4, pp. 170–179.

[30] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No. 1781/2006 (OJ EU L 141, 5.6.2015), pp. 1–18.

> compliance management and communication to prevent operations related to money laundering or terrorist financing.[31]

Detecting relevant risks, especially in relation to cyber security and criminal activities, can be quite a challenge for the private sector burdened with the obligation.[32] There are supranational and national risk assessment, sector-specific guidelines for supervisory bodies, and the internal rules of the service provider concerned, including risk-based internal procedures.[33] The implement of the supranational approach to risk identification is the task of the European Union in accordance with the IV. AML Directive.[34] The first Supranational Risk Assessment (SNRA) was adopted in 2017.[35] The aim of the report is to identify, analyse and evaluate the ML and TF risks at Union level. At this time the Commission set up the FinTech[36] Working Group to investigate the dangers of technological development, technology-enabled services and business models (e.g., digital currencies) in order to asset the dangers associated with them. In 2022, the European Commission adopted the third "Supranational Risk Assessment Report" of the risk of money laundering and terrorist financing affecting the internal market and in relation to cross-border activities.[37] The national legal framework will always depend on the development and ecosystem of the country

[31] Art. 35(1) III. AML Directive.

[32] B. Vogel, *Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing*, "Eucrim" 2022, No. 1, pp. 52–60.

[33] Zs. Papp (ed.), *Magyarázat a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról*, Budapest 2019, pp. 134–147.

[34] Art. 6(1) IV. AML Directive.

[35] COM (2017) 340 final.

[36] FinTech refers to technology-enabled and technology-supported financial services. Technology has the potential to facilitate access to financial services and to make the financial system more efficient "Reg Tech" is about adopting new technologies to facilitate the delivery of regulatory requirements.' See the definition in the first SNRA in 2017, COM (2017) 340 final, p. 9.

[37] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, COM (2022) 554 final, Brussels, 27 October 2022.

concerned. Therefore, countries have to take different approaches in the national risk assessment (NRA), a "one size fits all" solution to assessing money laundering – including cyber-laundering risks – is not feasible.[38]

4.3.2. REQUIREMENT TO REPORT SUSPICIOUS TRANSACTIONS AND THE ROLE OF THE FINANCIAL INTELLIGENCE UNIT (FIU)

The "risk-based approach" to combat money laundering was introduced with the 3rd AML Directive to replace the rules-based approach.[39] In accordance with the new approach, the current trends and typologies of money laundering must be taken into account.

Of central importance among the obligations imposed on actors in the financial and economic spheres is the reporting obligation with which service providers bring valuable information to the attention of the authority operating as a financial intelligence unit (Financial Intelligence Unit, FIU[40]). The reporting obligations means the information of the FIU, including the filing of a report on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases;

[38] See World Bank Group: National Money Laundering and Terrorist Financing Risk Assessment Toolkit, 2022, https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use (accessed on: 13.07.2023). See the FATF National ML/TF risk assessment: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Nationalmoneylaunderingandterroristfinancingriskassessment.html (accessed on: 13.07.2023).

[39] J. Grzywot, *Virtuelle…*, *op. cit.*, p. 93.

[40] In Hungary is the FIU a department of the National Tax and Customs Administration of Hungary (NTCA), delegated by the relevant legislation. See: https://pei.nav.gov.hu/ (accessed on: 2.08.2023). See: G. Simonka, *A magyar FIU és a pénzmosás elleni intézményrendszer a nemzetközi együttműködés tükrében*, Budapest 2015.

and providing the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law.[41] It is important to underlined that all suspicious transactions, including attempted transactions, shall be reported, regardless of the amount.

The main role of national FIU in the preventive combatting of money laundering must be highlighted. The 1st AML Directive in 1991 only required that credit and financial institutions should cooperate with "the authorities responsible for combating money laundering". This term was used as a generic term, but the Directive didn't contain detailed rules for financial information units. Under an explicit provision of the III. AML Directive in 2005, each Member State is required to establish an FIU in order to combat money laundering and terrorist financing effectively.[42] In accordance with the IV. AML Directive from 2015, each Member State shall establish an FIU in order to prevent, detect and effectively combat money laundering and terrorist financing.[43] The FIU shall be a central national unit that shall be responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. Each FIU shall be operationally independent and autonomous. It shall be able to obtain additional information from obliged entities. The competent authorities have to provide feedback to the FIU about the use made of the information provided. The Member States shall ensure that their FIUs have access to the financial, administrative and law enforcement information that they require to fulfil their tasks properly. Where there is a suspicion that a transaction is related to money laundering or terrorist financing, the FIU has to

[41] Art. 33 IV. AML Directive.

[42] Art. 21 III. AML Directive.

[43] Art. 32 IV. AML Directive. There are three basic types of financial information units: administrative, investigative or judicial. The FIU could be a hybrid institution too if the characteristics of the three basic types of FIU appear in a somewhat mixed way. See about more: G.A. Simonka: *A pénzügyi információs egység*, [in:] Zs. Papp (ed.), *Magyarázat a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról,* Közigazgatási és Jogi Kiadványok, Budapest 2019, p. 175.

be empowered to take urgent action to suspend or withhold consent to a transaction in order to analyse the transaction and disseminate the results of the analysis to the competent authorities. The FIU can take such action, at the request of an FIU from another Member State. The very important legal background in accordance with the cooperation between the authorities is Directive (EU) 2019/1153 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.

4.3.3. THE FIGHT AGAINST MONEY LAUNDERING BY CRIMINAL LAW

As mentioned above the AML measures of the European Union can be divided into two main categories, The other instrument system concerns criminal law. Nowadays, the penal codes of all EU member states regulate the crime of money laundering. It was codified from the beginning of the 1990s, although the EU regulations only required the prohibition of money laundering. The reason for this was the lack of criminal law competence of the European Communities (European Union).[44] The criminalisation obligation came into force only with the issuance of the 6th AML Directive.[45] The provisions of 6th AML Directive complement and reinforce the existing preventive measures. The aim is to enable more efficient and swifter cross-border cooperation between competent authorities.[46] It must be mentioned that the EU legislator recognised the importance

[44] See B. Udvarhelyi, *Az Európai Unió anyagi büntetőjog a Lisszaboni Szerződés után*, Budapest 2019, pp. 97–133; B. Udvarhelyi, *Kézikönyv az Európai Unió pénzügyi érdekeinek védelméről*, Budapest 2022, p. 63; B. Udvarhelyi, *Criminal law competences of the European Union before and after the Treaty of Lisbon*, "European Integration Studies" 2015, Vol. 11, No. 1, pp. 46–59.

[45] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (OJ EU L 284, 12.11.2018), pp. 22–30.

[46] Preamble 1, VI. AML Directive.

of action against cybercrime and therefore identified cybercrime among the list of predicate offences.[47]

The 6th AML Directive contains the repressive measures for combating money laundering and lays down minimum standards for criminal offenses and sanctions.[48] The Directive, which establishes minimum rules for the member states regarding the crime and the legal consequences of money laundering, was a milestone of outstanding importance on the EU scene of the fight against money laundering. This legislative act aims to combat money laundering through criminal law and to facilitate cross-border cooperation between competent authorities and complement the preventive measures regulated in IV. AML/CTF Directive (EU) 2015/849 in force.[49]

4.4. New Developments in the European Union

4.4.1. ACTION PLAN OF THE EUROPEAN COMMISSION 2020 AND LEGISLATIVE PACKAGE 2021

It must be highlighted that the EU's anti-money laundering framework began to develop dynamically following the adoption in 2020 of the "Action Plan for a comprehensive Union policy on preventing

[47] Cybercrime including any offence set out in Directive 2013/40/EU of the European Parliament and of the Council. See the definition of "criminal activity": Art. 2(1) VI AML Directive. It must be mentioned that it was the only crime which is not listed in the categories of offences in the 40 Recommendations of the FATF and the Warsaw Convention of the Council of Europe.

[48] Art. 1(1) VI. AML Directive.

[49] See: J. Jacsó, *Gondolatok az Európai Unió pénzmosás elleni büntetőpolitikájáról a hatodik Pénzmosás elleni uniós irányelv tükrében*, [in:] P. Bárd, A. Borbíró, K. Gönczöl (eds.), *Kriminológia és kriminálpolitika a jogállam szolgálatában. Tanulmányok Lévay Miklós tiszteletére*, Budapest 2019, pp. 401–411; J. Jacsó, B. Udvarhelyi, *The fight against money laundering in Hungary*, [in:] Á. Farkas, G. Dannecker, J. Jacsó (ed.), *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, pp. 295–309.

money laundering and terrorism financing".[50] The action plan builds on six pillars, which primarily cover preventive measures, but also affect criminal law.

On 20 July 2021, the Commission presented a package consisting of four legislative proposals to strengthen the EU AML/CFT provisions, as follow:

- AMLA Regulation: Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism;[51]
- New Regulation on AML/CFT: Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;[52]
- New Directive on AML/CFT: Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.[53] It is important

[50] Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06, C/2020/2800 (OJ C 164, 13.5.2020), pp. 21–33.

[51] Proposal for a Regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No. 1093/2010, (EU) 1094/2010, (EU) 1095/2010, COM (2021) 421 final, Brussels, 20 July 2021. See more about the AMLA: J. Jacsó, *New developments in the fight against money laundering, in particular the Commission's 2021 proposal with special regard to the Anti-money laundering Authority (AMLA)*, [in:] Á. Farkas, G. Dannecker, J. Jacsó (ed.), *External, internal and criminal investigations of criminal offences affecting the financial interests of the European Union,* Budapest 2022, pp. 467–481.

[52] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, COM (2021) 420 final, Brussels, 20 July 2021.

[53] Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, COM (2021) 423 final, Brussels, 20 July 2021.

to emphasise that the Directive will replace the 4th AML Directive 2015/849/EU. The new Directive will contain a provision that requires national implementation contrary to the rules in the new *Regulation on AML/CFT* (for example, rules on national supervisions and Financial Intelligence Units of the Member State);

- Reform of the Regulation on Transfers of Funds (Regulation 2015/847):[54] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets (recast).[55] This proposal was the first to be adopted by the EU legislator in 2023.

4.4.2. AMENDMENTS OF THE IV. AML DIRECTIVE TO PREVENT CYBER-LAUNDERING

The EU legislator recognised that it is important to ensure that Union legislative acts on financial services comply with the digital age. The first definition of virtual currency on the level of the EU was established by the 5th AML Directive in 2018. Before the amendment of the 4th AML Directive, providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers, which didn't fall under the Union's obligation to identify suspicious activity. Therefore, criminals were able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. Therefore, it became necessary to extend the scope of the 4th AML Directive so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet

[54] IV. AML Directive.

[55] Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast) COM (2021) 422 final, Brussels, 20 July 2021.

providers.[56] However, the EU legislator was also aware that "a large part of the virtual currency environment will remain anonymous because users can also transact without such providers".[57] "Virtual currencies" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically. We can see that the EU legislator refrained from using the term "crypto" and used the term "virtual currency".

The latest development in the recent past was the amendment of the IV. AML Directive by the Regulation Transfer of Funds (TFR[58]), which extended the scope of the directive to crypto-asset service providers. With this amendment, the EU legislator complies with the FATF Travel Rule (Recommendation No. 15). In addition, in 2023, the European Union adopted for the first time a harmonised regulatory framework for the crypto-asset market (Regulation (EU) 2023/1114 on Markets in Crypto-Assets, (MiCA[59]). The aim of MiCA is the establishment of uniform rules for issuers of crypto-assets that have not been regulated before by other European Union financial services acts[60] and for providers of services in relation to such crypto-assets (crypto-asset service providers).[61] These service

[56] Preamble 8, V. AML Directive.

[57] Preamble 9, V. AML Directive.

[58] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, OJ EU L 150, 9.6.2023, pp. 1–39. (TRF Regulation).

[59] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ EU L 150, 9.6.2023), pp. 40–205 (hereinafter: MiCA Regulation).

[60] One group of crypto assets was classified as a financial institution and was regulated before, see: Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ 173, 12.6.2014), p. 349.

[61] See: summarised about the main regulations of MiCA, https://eur-lex.europa.eu/EN/legal-content/summary/european-crypto-assets-regulation-mica.html (accessed on: 03.06.2023).

providers must comply with a number of obligations. The scope of MiCA "applies to natural and legal persons and certain other undertakings that are engaged in the issuance, offer to the public, and admission to trading of crypto-assets or that provide services related to crypto-assets in the Union."[62] Crypto-assets are one of the main applications of distributed ledger technology (DLT). In accordance with the provision of MiCA, "crypto-asset" means a "digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology".[63] It must be underlined that the MiCA regulation applies to any new player in the crypto-ecosystem involved in the issuance.[64]

4.5. Summary and Conclusion

The scope of legal framework of the EU became wider and wider, the latest legal documents even cover the crypto asset service providers and crypto assets. The EU legislator used the term crypto whereas the FATF recommends the term "virtual", but they are synonymous. With the new EU legal framework, every cryptocurrency-related business has to adhere to the same AML/CFT rules as other financial service providers. The traditional strategy to "follow the money" could be changed in the digital age to "follow the virtual asset", which could be a rule of thumb in the effort to combat the new form of money laundering – cyber-laundering.

The cross-border nature of money laundering and cyber-laundering is a significant factor that makes it difficult to combat these crimes and to identify the perpetrators. In the fight against money laundering, the cooperation of several institutions is very important at the national as well as the international level. The proper

[62] Art. 2(1) MiCA Regulation.
[63] Art. 3(1) pt 5 Regulation (EU) 2023/1114.
[64] See: https://www.cssf.lu/en/2023/07/regulation-on-markets-in-crypto-assets-mica-and-regulation-on-information-accompanying-transfers-of-fund-and-certain-crypto-assets/ (accessed on: 03.08.2023).

application of preventive measures in practice can make a major contribution to the investigation and prosecution of money laundering cases. It requires the use of diverse tools of international cooperation and tools to secure and transfer data without delay. The fight against money laundering is characterised by the so-called multi-institutional approach, which could be employed in the fight against cybercrime generally. It is very important to point out that preventive measures are of particular importance in the fight against cyber-laundering, and crypto assets providers could as well play a decisive role.

This proposal package of the European Commission has been an important step in the field of harmonisation of anti-money laundering framework in the EU. With the adoption of the new AML/CFT rulebook, the EU regulatory and enforcement framework will be more uniform. The legal framework of harmonised and comprehensive anti-cyber laundering measures are an indispensable tool for combating cybercrime, in which preventive tools are of decisive importance. However, it is crucial that all actors in the fight against cyber-laundering have sufficient expertise, for which appropriate training is essential.[65]

REFERENCES

Brandl, R., Bülte, J., *Kryptowährungen/-assets – Geldwäsche und Terrorismusbekämpfung –Perspektive Sorgfaltsverpflichtete*, [in:] Leitner, R., Brandl, R. (eds.), *Finanzstrafrecht 2022 Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht*, Vienna 2023, pp. 105–122.

Bussmann, K.-D., Vockrodt, M., *Geldwäsche-Compliance im Nicht-Finanzsektor: Ergebnisse aus einer Dunkelfeldstudie*, "Compliance Berater" 2016, No. 5.

Farkas, Á., Dannecker, G., Jacsó, J., *Conclusion and recommendation of the project*, [in:] Farkas, Á., Dannecker, G., Jacsó, J. (eds.), *External, internal and criminal investigations of criminal*

[65] Á Farkas, G. Dannecker, J. Jacsó, *Conclusion and recommendation of the project*, [in:] Á. Farkas, G. Dannecker, J. Jacsó (ed), *External…*, *op. cit.*, p. 498.

offences affecting the financial interests of the European Union, Budapest 2022, pp. 490–502.

Grzywot, J., *Virtuelle Kryptowährungen und Geldwäsche*, Internetrecht und Digitale Gesellschaft, Band 15, Berlin 2019.

Jacsó, J., *A pénzmosás*, [in:] Farkas, Á. (ed.), *Fejezetek az európai büntetőjogból*, Miskolc 2017.

Jacsó, J., *Gondolatok az Európai Unió pénzmosás elleni büntetőpolitikájáról a hatodik Pénzmosás elleni uniós irányelv tükrében*, [in:] Bárd, P., Borbíró, A., Gönczöl, K. (eds.), *Kriminológia és kriminálpolitika a jogállam szolgálatában. Tanulmányok Lévay Miklós tiszteletére*, Budapest 2019, pp. 401–411.

Jacsó, J., *New developments in the fight against money laundering, in particular the Commission's 2021 proposal WITH special regard to the Anti-money laundering Authority (AMLA)*, [in:] Farkas, Á., Dannecker, G., Jacsó, J. (ed.), *External, internal and criminal investigations of criminal offences affecting the financial interests of the European Union*, Budapest 2022, pp. 467–481.

Jacsó, J., Udvarhelyi, B., *A Bizottság új irányelvjavaslata a pénzmosás elleni büntetőjogi fellépésről az egyes tagállami szabályozások tükrében*, "Miskolci Jogi Szemle" 2017, No. 2, pp. 43–44.

Jacsó, J., Udvarhelyi, B., *The fight against money laundering in Hungary*, [in:] Farkas, Á., Dannecker, G., Jacsó, J. (eds.), *Criminal law aspects of the protection of the financial interest of the EU: with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*, Budapest 2019, pp. 295–309.

Langlois, D., *The Revision of the EU Framework on the Prevention of Money Laundering*, "Eucrim" 2013, No. 3.

Leslie, D.A., *Legal Principles for Combatting Cyberlaundering*, New York 2014.

Mauma, Ph., Maute, L., Fromberger, M., *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, München 2020.

Met-Domestici, A., *The Fight against Money Laundering in the EU – The Framework Set by the Fourth Directive and its Proposed Enhancements*, "Eucrim" 2016, No. 4.

Met-Domestici, A., *The Reform of the Fight against Money Laundering in the EU*, "Eucrim" 2013, No. 3.

Papp, Zs. (ed.), *Magyarázat a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról*, Budapest 2019.

Rückert, Ch., *Phänomenologie*, [in:] Mauma, Ph., Maute, L., Fromberger, M., *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coin Offerings*, München 2020, pp. 527–536.

Simonka, G., *A magyar FIU és a pénzmosás elleni intézményrendszer a nemzetközi együttműködés tükrében*, Budapest 2015.

Udvarhelyi, B., *Az Európai Unió anyagi büntetőjog a Lisszaboni Szerződés után*, Budapest 2019.

Udvarhelyi, B., *Criminal law competences of the European Union before and after the Treaty of Lisbon*, "European Integration Studies" 2015, Vol. 11, No. 1, pp. 46–59.

Udvarhelyi, B., *Kézikönyv az Európai Unió pénzügyi érdekeinek védelméről*, Budapest 2022.

Udvarhelyi, B., *Pénzmosás elleni küzdelem az Európai Unióban*, [in:] *Studia Iurisprudentiae Doctorandorum Miskolciensium – Miskolci Doktoranduszok Jogtudományi Tanulmányai*, Tomus 12., Gazdász-Elasztik Kft., Miskolc 2013, pp. 455–471.

Vogel, B., *Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing*, "Eucrim" 2022, No. 1, pp. 52–60.

Zéman, Z., Hegedűs, M., *Pénzmosás mint negatív gazdasági tényező az Európai Unióban*, "Belügyi Szemle" 2023, No. 5, pp. 885–904.