

THE DIGITAL ERA AND ITS IMPACT ON MONEY LAUNDERING

ALEXANDRU FRĂSILĂ

Bucharest University of Economic Studies

Bucharest, Romania

avocat.frasila@gmail.com

Abstract

This article analyses, from an interdisciplinary and contextual perspective, the issue of money laundering, with a particular focus on its occurrences in the digital context, especially via the use of online platforms – known in the legal literature as cyber laundering. The article presents the main ways in which this type of criminal behavior materializes, such as cryptocurrency transactions, online banking, online auctions, and online gambling, thus illustrating the methods used by cybercriminals in order to cover up the illicit origin of the funds.

The issue of money laundering portrays, from an economical perspective, a facet of the informal, covert, underground economy, which legally translates into a series of operations aiming to confer an illusion of legality to the profits resulting from criminal activity. The effects of this scourge are destructive for the harmonious functioning of society, distorting the market economy and the competitive market, while generating financial instability and leading to an increase in corruption and organized crime.

Within the context of the digital era, this article explores the impact of technology on the evolution of the practice of money laundering and discusses the new methods used in such criminal activity, while simultaneously dealing with the way in which the new technologies, such as artificial intelligence, can be used in order to prevent and counter the practice of money laundering.

Keywords: *money laundering; artificial intelligence; cybercrime; cyber laundering; crypto-assets.*

JEL Classification: K14; K24; K42.

1. INTRODUCTION

The digital era we are living in, is a period in which new technologies, such as the Internet, computers, artificial intelligence and communication networks, have become frequent in social, economic, cultural and institutional life and it influences the way people communicate, work, learn and access information.

Technological progress brings numerous benefits and facilitates the development of contemporary society, but at the same time, it creates new criminal opportunities. Crimes committed in cyberspace have been defined by the Council of Europe, through the Convention on Cybercrime (2001), as “those

committed against the integrity, availability and confidentiality of information systems and telecommunications networks or those committed by using them to commit traditional crimes” (Niță *et al.*, 2024, p. 572).

The crime of money laundering is associated with organized crime and it affects the social and economic order and the Rule of law. Criminal activity undermines the economy, affects trade activities, harms the system of free competition, supports the activities of organized crime and obstructs the proper administration of justice.

The specialised doctrine considers that the prosecution of money laundering activities and the seizure of the proceeds of the crime, can be regarded as a new strategy in the fight against organized crime, as it targets directly the engine of organized crime development (the money or goods obtained from criminal activities and the funds used for criminal purposes) (Jurj and Șaguna, 2022, p. 7).

The fight against money laundering has a dual objective, namely preventing the development of organized crime by depriving them of funds, as well as creating a solid, integral and stable economic and financial system. (Dobrescu and Cucu, 2023, p. 15)

From a legal perspective, money laundering is defined as “the operation of disguising profits resulting from committing crimes, transferring money that came from illicit activities, through various transactions with the role of concealing their real source and origins” (Urda, 2016, p.116). From an economical perspective, it represents a “way of manifestation of the informal, hidden, underground economy” (Hotca, 2019, p. 10).

According to the Council of the European Union (2023), it is estimated that between 715 billion euros and 1.87 trillion euros are laundered annually, which is between 2% and 5% of the Global GDP. In this context, it can be stated that the phenomenon of money laundering currently represents one of the most serious problems the global economy is facing.

2. CYBERLAUNDERING AND MODERN TECHNOLOGIES

The impact of technology on contemporary society has facilitated the emergence of new techniques and methods of money laundering, enclosed in the concept of cyber laundering, which refers to “the use of the Internet in cyberspace to conceal the illicit origin of values money or other assets) obtained from criminal activities” (Coman, 2022, p. 118).

According to the specialized literature, cyber laundering represents “the use of an information system in order to carry out a transaction involving property or profit, whether tangible or intangible and originating from criminal activities” (Leslie, 2014, p. 56, cited in Moise, 2016a, p. 278).

Investigating money laundering in cyberspace involves proving the existence of a predicate offense from which the illicit funds were obtained, demonstrating the activity through which the criminal proceeds were hidden, for example,

performing a transaction through an information system, as well as proving knowledge or suspicion regarding the illicit origin of the funds, and the intentional use of these illegal funds in various transactions, carried out in order to create an appearance of legality (Moise, 2016a, p. 279).

2.1. Crypto-assets

Electronic payment systems can be characterized as one of the most widely used money laundering activities. In the case of multiple transfers made in order to hide the illicit origin of the funds, the payor and the real receiver may be one and the same person, while using false identities or intermediary people to make these transfers (Jurj and Şaguna, 2022, p. 146).

While efforts are made to provide information regarding the payor and the receiver in electronic money transfers, there are difficulties in investigating money laundering cases when these systems include not only banks, but also currency exchange houses or other financial institutions that have multiple access points and that facilitate anonymous exchanges and rapid transfers (Jurj and Şaguna, 2022, p. 146).

The National Office for the Prevention and Combating of Money Laundering in Romania (2025) indicates in a report the existence of a significant difficulties in the efforts made to prevent and combat money laundering in the field of crypto-asset transactions, due to the virtual characteristics, which allow anonymity, as well as the rapid and global transfer of value

Europol has drawn attention to the use of crypto-assets for the purpose of making payments connected to corruption and money laundering activities, being an area that generates real concern, due to the absence of a common regulatory framework and the level of anonymity that these products offer (Europol, 2021). Specialised studies reveal that the efforts to combat money laundering at the global level are only 0.1% away from a total failure (Cassara, 2017, p. 5), especially in the new era of crypto-assets (Jurj and Şaguna, 2022, p. 1).

At European level, constant efforts are being made to adapt the legislation to the new challenges determined by technological evolution, which has offered new criminal opportunities, such as terrorist financing, drug trafficking, tax evasion and other illegal activities in the financial sphere.

In Romania, the regulatory framework managing the prevention and the combat of money laundering and terrorist financing, Law no. 129/2019 (Official Gazette no. 589/2019), was recently amended by the legislator through Government Emergency Ordinance no. 10/2025 (Official Gazette no. 225/2025), by transposing the requirements of Regulation (EU) 2023/114 on crypto-asset markets into national legislation. The main changes that have been introduced relate to: updating of terminology and the expansion of definitions, the classification of crypto-asset service providers as financial institutions, imposing on them obligations similar to those of banks or investment firms, the clarification of certain supervisory and control powers incumbent on the National Bank of

Romania and the Financial Supervisory Authority, as well as additional customer due diligence obligations (NOPCML, 2025).

2.2. Online banking

Online banking involves the use of the internet, by financial institutions, in order to conduct regular banking operations. It is one of the most frequent methods used in cyber laundering activities, in cases of opening online bank accounts and conducting multiple transactions, where the operation model involves the technique of smurfing (Coman, 2022, p. 118).

Smurfing is carried out at the placement stage of the money laundering process and is used to avoid reporting and bank record-keeping requirements (Moise, 2016b, pp. 317-325).

Large-value transactions between two accounts are often automatically reported in accordance with the legal regulations of each state. As a result, large amounts are divided into smaller transactions and transferred through multiple money couriers, called “smurfs”. This method makes it more difficult to detect illicit money flows, because the origin of the funds is hidden and small-value transactions appear less suspicious (Deprez *et. al.*, 2025, p. 1).

For example, the amount of 100.000 euros coming from drug traffic is split among 15-20 transactions (all under the mandatory reporting threshold), all made by different individuals (“smurfs”), who make deposits at different banks. In this way, the bank does not immediately report the transactions and the money is subsequently transferred to various accounts belonging to the criminal.

2.3. Online gambling

Cyber Laundering through gambling, presumes laundering money obtained from illegal activities within online casinos. In this context, an existing online gambling website can be used, or creating a new website for cyber laundering, which would imply more risks (Golonka, 2024, p. 218)

The specialised literature has presented a situation where a cyber launderer creates a gambling website and distributes the illegal funds through the smurfing technique. In this context, it is irrelevant whether the cyber launderer wins or loses at online gambling, as all funds obtained from illegal activities ultimately return to the cyber launderer (Moise, 2016a, p. 281).

The use of gambling or sports betting services in money laundering operations is easy, especially due to the cross-border and anonymous nature of the internet, as well as the lack of international consolidated regulations, in some countries gambling being considered a legal activity, and in other states illegal (Coman, 2022, p. 118).

2.4. Illustrative cases from judicial practice

In Romania, the authorities identified and prosecuted an organized criminal group that carried out activities specific to the notion of cyber laundering, using online banking transactions and crypto-asset transactions in their criminal activity, in order to hide the illicit origin of the criminal proceeds (Vâlcea Tribunal, Decision no. 43/2025).

The members of the group posted false advertisements for the sale of movable property, especially cars, on specialized websites, such as the online platform eBay, property that they did not actually own, illegally introducing in this way, computer data that was not in accordance with the truth and thus harmed several people in the European Union through acts of deception. At the same time, the members of the criminal group or intermediaries opened bank accounts in the country and abroad, using false documents, where the deceived parties transferred the amounts of money in order to purchase the goods, without receiving the agreed consideration or the refunds. Subsequently, the members of the organized criminal group recruited other people, with a precarious financial situation and a low level of education, in order to have them open bank accounts with real data, so they can transfer the criminal proceeds on a regular basis. Ultimately, the sums of money were withdrawn from bank cashiers or ATMs by the intermediaries and used to purchase crypto assets, the intended purpose being to launder the proceeds of fraud.

In South Africa, members of an organized crime group conducted multiple crypto-asset transactions for criminal purposes, successfully transferring 108,352,900 U.S. dollars (equivalent to 11,960 bitcoins) abroad. Initially, before purchasing the virtual assets, the cyber launderers carried out multiple layering of the funds, depositing the money into accounts opened at various financial institutions. Subsequently, the amounts were transferred via electronic payments to various accounts, and finally were purchased from local virtual asset service providers (VASPs). One of these local providers submitted suspicious transaction reports, due to the doubts raised by the purchase of large amounts of bitcoins by various individuals and their rapid transfer to virtual asset service providers in foreign jurisdictions. Also, many of the wallet holders had the same home address, and most of the addresses related to the virtual assets were accessed from the same IP address, which created suspicion regarding the use of "money mules" for money laundering purposes (FATF, 2020, p.6).

3. ARTIFICIAL INTELLIGENCE

In addition to the methods already established in the procedures for preventing, detecting, investigating and combating money laundering, technological advances outline the possibility of using a new tool, namely artificial intelligence, which can be a determining factor in streamlining the processes (Urdă, 2016).

An artificial intelligence system is defined as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (Regulation UE 2024/1689, p. 46).

In theory, artificial intelligence must be viewed from two perspectives, in the sense that it can be "an invaluable tool for criminal prosecution bodies and forensic specialists, but at the same time it is a sophisticated and extremely effective weapon in the hands of criminals" (Niță *et al.*, 2024, p. 595).

The integration of artificial intelligence and machine learning technologies can significantly contribute to increasing the efficiency of financial institutions, reducing the time and costs generated by manual human inspections (Basu and Tetteh, 2024, p. 5).

The efficiency of artificial intelligence mechanisms is presented in the specialized literature, which could play an essential role in procedures for preventing and combating money laundering by automating the verification of suspicious transactions, given the huge volume of data reported daily (Coman, 2022, p. 120).

For example, based on customers' transactional behaviour history, each customer can be given a money laundering benchmark score, alerts for suspicious or unusual transactions being generated if the customer's current behaviour is different from their previous transactional pattern (Basu and Tetteh, 2024, p. 5).

In the case of money laundering, the analysis criteria cannot be limited to certain distinct transactions, it requires the assessment of the entire factual context (people, the relationships between them, the complex system of exchanges), based on the principle of "follow the money" (Agapito *et al.*, 2021, cited in Coman, 2022, p. 122). In this regard, it is stipulated that "the quality of investigations and the implementation of appropriate sanctions can never be limited exclusively to the decision of automated information systems".

However, we cannot forsake the risks generated by the use of artificial intelligence and machine learning technologies. A report by the International Monetary Fund (IMF) draws attention to the significant threat that artificial intelligence can constitute to the stability of the entire financial system. Among the main risks are the violation of data confidentiality, the difficulty of explaining decisions generated by artificial intelligence (lack of transparency) and the vulnerabilities generated in cybersecurity (Basu and Tetteh, 2024, p. 6).

The use of AI by law enforcement is also constrained by a number of legal, ethical and technical limitations. Issues related to data privacy and risks of excessive surveillance create a "tension between the need for security and the protection of fundamental human rights" (Niță *et al.*, 2024, p. 596).

Artificial intelligence can generate significant risks and it can affect public interests and the fundamental rights protected by European Union regulations, causing material or moral damage, with physical, psychological, social or economic impact (Regulation EU 2024/1689).

According to a report generated by the European Parliament, on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, it is emphasised that Member States need to make sure customers are informed when they are subject to the use of AI and that citizens and consumers are provided with simple, effective and easily accessible complaint and redress procedures in order to allow them to effectively defend their rights in Report 2020/2016 (European Parliament, 2021). In regard to the integration of technology into the judicial system, the general option that I also support is that "digitalization should be neither total nor completely mandatory" (Ciurea, 2022, p. 179).

4. CONCLUSIONS

At the European level, as well as in Romania, we can observe the consistent steps taken by the legislator to improve the legal provisions in the matter, in order to streamline the procedures for preventing and combating the phenomenon of money laundering. In the context of technological evolution, it is imperative that the legislators, who are constantly forced to adapt to the challenges generated by the emergence of new money laundering techniques, demonstrate due diligence.

In addition to the traditional money laundering techniques, such as the purchase of real estate and movable assets (luxury objects, precious metals) or the falsification of tax documents, cyber launderers are currently using the internet to conceal the criminal proceeds, through operations with crypto-assets, online banking or online gambling.

Given that modern technologies are used for criminal purposes; to camouflage the illicit origin of sums of money or assets, it is necessary for judicial bodies to adapt and use new technologies to identify and combat cyber laundering activities in a timely manner. The expanding evolution of artificial intelligence outlines the need for its consolidation into the judicial system and law enforcement, as it can bring real contributions in terms of efficiency.

The use of artificial intelligence-based systems can represent a real support in certifying suspicious transactions, nonetheless, the human factor of decision-making and control cannot and should not be completely replaced by artificial intelligence-based systems.

In order to avoid errors and misjudgements and to ensure the security and safety of economic transactions, to respect the fundamental rights, such as the right to privacy and the protection of personal data, it is necessary to have a balanced approach that combines technology and manual oversight.

It is essential to create a consistent regulatory framework at international level, regarding the conditions and manner in which artificial intelligence is used and controlled, and the persons who are the object of the use of artificial intelligence must be informed and have at their disposal simple and accessible legal complaint mechanisms.

I believe that the use of artificial intelligence in the act of justice should be limited only to outputs in the form of predictions, content and recommendations, without allowing decisions to be made that could harm fundamental human rights.

References

- 1) Basu, D. and Tetteh, G.K. (2024). Using Automation and AI to Combat Money Laundering. *FRIL White Paper Series*. University of Strathclyde. [online] Available at: https://www.strath.ac.uk/media/departments/accountingfinance/fril/whitepapers/Using_Automation_and_AI_to_Combat_Money_Laundering.pdf [Accessed 24.06.2025].
- 2) Cassara, J.A. (2017). *Countering International Money Laundering Total Failure is „Only a Decimal Point Away”*. [online] Available at: <https://thefactcoalition.org/wp-content/uploads/2017/08/Countering-International-Money-Laundering-Report-August-2017-FINAL.pdf> [Accessed 24.06.2025].
- 3) Ciurea, A. (2022). *The Digital Age (III). Ethics, Law and Responsibility – an indispensable triptich in AI regulation*. *Universul Juridic*, no. 10, pp. 163-179. [online] Available at: <https://www.ceeol.com/search/article-detail?id=1079672> [Accessed 24.06.2025].
- 4) Coman, V. (2022). Using artificial intelligence to investigate and prevent money laundering. *Curierul Judiciar*, no. 2, pp. 118-123., [online] Available at: <https://www.ceeol.com/search/article-detail?id=1021398> [Accessed 24.06.2025].
- 5) Council of the European Union. (2023). *Anti-money laundering: Improving EU rules*. [online] Available at: <https://www.consilium.europa.eu/ro/infographics/anti-money-laundering/> [Accessed 24.06.2025].
- 6) Deprez, B., Baesens, B., Verdonck, T. and Verbeke, W. (2024). *GARG-AML against Smurfing: A Scalable and Interpretable Graph-Based Framework for Anti-Money Laundering*. arXiv preprint. [online] Available at: <https://arxiv.org/abs/2506.04292> [Accessed 24.06.2025].
- 7) Dobrescu, A. and Cucu, A. (2023). Combating money laundering and terrorist financing in the EU. *Revista Consultant Fiscal*, no. 2, pp. 10-15. [online] Available at: <https://www.ceeol.com/search/article-detail?id=1179598> [Accessed 24.06.2025].
- 8) European Parliament (2021). *Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI))*. [online] Available at: https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html [Accessed 24.06.2025].
- 9) 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 648/2012. *Official Journal of the European Union*, L 150, 9.6.2023, pp. 40–173. [online] Available at: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng> [Accessed 24.06.2025].

- 10) Europol (2021). *EU SOCTA 2021, Serious and organized crime threat assessment - A corrupting influence: The infiltration and undermining of Europe's economy and society by organized crime*. [online] Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf [Accessed 24.06.2025].
- 11) FATF Financial Action Task Force (2020). *Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing*. [online] Available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf> [Accessed 24.06.2025].
- 12) Golonka, A. (2024). Cyberlaundering in the Era of Modern Technologies. *Przełąd Policyjny*, no. 2, pp. 205-224. [online] Available at: <https://www.ceeol.com/search/article-detail?id=1341905> [Accessed 24.06.2025].
- 13) Hotca, M.A. (2019). *Spălarea banilor. Evoluția, conținutul și contrafacerea fenomenului*. [online] Available at: <https://www.juridice.ro/essentials/3162/spalarea-banilor-evolutia-continutul-si-contracacarea-fenomenului>. [Accessed 24.06.2025].
- 14) Jurj, R. and Șaguna, D.D. (2022). *Spălarea banilor, Teorie și practică judiciară*, Ed. 5. București: Ed. C.H. Beck.
- 15) Moise, A.C. (2016a). Aspects related to cyberlaundering investigation. *Curierul judiciar*, no. 5, pp. 278-283. [online] Available at: <https://www.ceeol.com/search/article-detail?id=553094>. [Accessed 24.06.2025].
- 16) Moise, A.C. (2016b). Techniques Frequently Used in Money Laundering Crimes. *International Conference of Law, European Studies and International Relations*, no. IV, pp. 317-325. [online] Available at <https://www.ceeol.com/search/article-detail?id=824537> [Accessed 24.06.2025].
- 17) NOPCML National Office for the Prevention and Control of Money Laundering, (2025). *Ghid privind indicatori de suspiciune și tipologii de spălare a banilor în domeniul criptoactivelor*, Ediția a II-a, [online] Available at: <https://www.onpcsb.ro/uploads/articole/attachments/67eb8f930d612007345948.pdf>. [Accessed 24.06.2025].
- 18) Niță, N., Apreutesei, C. and Său, C. (2023). Cybercrime through the lens of artificial intelligence. *Acta Universitatis George Bacovia. Juridica*, no. 2, pp. 569-601. [online] Available at: <https://www.ceeol.com/search/article-detail?id=1301327>. [Accessed 24.06.2025].
- 19) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 1689, 13.6.2024. [online] Available at: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R1689> [Accessed 24.06.2025].
- 20) Vâlcea Tribunal (2025). *Decision no. 43/2025 of 27 March 2025. Case code: RJ72867g8d8*. [online] Available at: <https://www.rejust.ro/juris/72867g8d8> [Accessed 24.06.2025].
- 21) Urdă, O. (2016). Money laundering offence – European and domestic regulations. *Revista Universul Juridic*, no. 5, pp. 114-125. [online] Available at: https://www.universuljuridic.ro/wp-content/uploads/2016/08/06_Revista_Universul_Juridic_nr_05-2016_PAGINAT_BT_O_Urda.pdf [Accessed 24.06.2025].