Multidiszciplináris tudományok, 13. kötet, 2. sz. (2023), pp. 197-208 **https://doi.org/10.35925/j.multi.2023.2.18**

THE IMPACT OF DIGITALISATION ON MONEY LAUNDERING

Judit Jacsó
habilitated associate professor, University of Miskolc, Institute of Criminal Justice, Department of Criminal Law and Criminology
3515 Miskolc-Egyetemváros, e-mail: judit.jacso@uni-miskolc.hu

Vivien Cintia Vámosi
PhD student, University of Miskolc, Institute of Criminal Justice, Department of Criminal Law and Criminology
3515 Miskolc-Egyetemváros, e-mail: vivien.vamosi@uni-miskolc.hu

Abstract

The crime of money laundering poses many dangers. It is used by a significant proportion of criminals to try to hide the proceeds of crime. This is mostly done through the banking system, but digitalisation is increasing the variety of options available to criminals. Money laundering through financial institutions is one of the most common forms of money laundering, but money laundering in the virtual space is also becoming increasingly common. Cryptocurrencies and crypto-assets are the main threat in this respect, as one person can have several virtual "wallets" and there is a high degree of anonymity. This increases latency and makes it almost impossible for the authorities to trace the origin of assets.

Keywords: *money laundering, digitisation, money mule, cryptocurrency*

1. Introduction

Money laundering is one of the most significant criminal offences today and covers a complex phenomenon. In general terms, it can be defined as the act of disguising the origin of illegally obtained proceeds. (Ambrus, 2021.) It includes any conduct by which the offender aims to conceal the origin of the proceeds of an illegal act in order to make them appear legal states that money laundering is a punishable offence of laundering money or property of monetary value derived from other offences through activities that are vulnerable to money laundering and that the purpose of the Act is to prevent the support of terrorism by money or property of monetary value. (Act LIII of 2017 Preamble)

The individuals and institutions involved in money laundering are diverse, often engaging in complex transactions that are (or appear to be) legal in themselves, in order to hide the profits made. This allows illicit proceeds to be presented to the authorities as legal, so that they can be used for further legal and illegal activities (Ambrus, 2021). Money laundering, unlike many other crimes, consists of a number of seemingly legal steps. For example, a bank account opening, a wire transfer or even a cryptocurrency transaction. However, the money that is moved in this way comes from a previous criminal offence. The offence of money laundering itself does not directly harm anyone, but it is still morally reprehensible because it is always preceded by the commission of some other criminal offence as an accessory offence. (Jacsó, 2021).

The money laundering process involves three main steps. The first is always the placement, which is not an act in a predetermined place. Criminals often employ unsuspecting individuals, who are not

otherwise connected to them, to deposit illicit assets in financial institutions, for which they also receive a fee. These persons are the so-called money couriers, who will be discussed in more detail later in this paper. At this stage, too, the identity of the original payer remains anonymous, even if the money transmitter is unmasked. The next step is layering, where the origin of the money deposited is removed and separated from the source. The money thus hidden becomes part of the legal economy through a series of reuses. The last main step is integration, where the criminal wealth is transferred into a legal business as a form of revenue, where it appears as a legally acquired asset through the falsification of accounting records. Tax is paid on the resulting profits and the offenders then usually receive what now appears to be legal assets as dividends. (Lentner et al., 2017)

Money laundering is an ever-changing offence, influenced not only by the perpetrators but also by technological developments. This has a fundamentally negative impact on the way the crime changes. As money flows are now almost unrestricted, financial sector actors are also engaged in complex work, carrying out countless financial transactions. This makes the work of the authorities much more difficult. This makes the fight against money laundering a major responsibility for supervisory bodies. Action can only be taken at international level, for which a harmonised legislative environment and enforcement are essential. (Ambrus, 2021)

2. The advent of digitalisation

One of the most inescapable areas of today's world is the development of technology and the rise of digitalisation. In the legal world, this initially meant a simpler, paperless way of doing business, where it could be done more quickly without the need for printing and postal services. However, there was soon a demand from clients for electronic forms and the use of structured information. This is when they started to look at how legal processes could be automated.

Thanks to digitalisation, new procedures have emerged in the justice system, which have changed the way different areas operate and work. This has had an impact on the procedures and the situation of clients. The traditional written form has changed, and digital contracts and evidence are taking over in legal transactions, which pose different problems. Electronic procedures have increased the role of forms, which, if not filled in correctly, can also present a number of risks. The work of lawyers has also changed, with the emphasis now being placed on writing, which requires a much more precise and accurate approach. (Nagy, 2020)

The last few years have also seen technological change in many areas of the economy. These changes have also had an impact on financial flows and financial infrastructure, which are increasingly dependent on information systems. Digitalisation processes are having a greater and greater impact on the banking sector and its competitiveness. (Mezei, 2019) Increasingly, bank customers are choosing a financial institution to manage their accounts, investments and loans where they can manage their finances from the comfort of their home, by phone or electronically, rather than in person. For this reason, the banking sector needs to evolve continuously. While it was previously unthinkable for someone to open a bank account or apply for a personal loan in a few minutes from home in the evening by taking a selfie and a photo of their documents, today, thanks to digitalisation, this is possible at most financial institutions. However, this technical freedom brings with it a number of risks which financial institutions are not yet fully prepared to face because of the competitive situation. The use of cash is also becoming increasingly marginalised, and even in the context of the epidemic situation in recent years, people have been urged to avoid using it as much as possible in order to prevent infections and prevent their spread. Partly as a result of this, people are now more willing to use electronic payment methods such as bank transfers,

credit cards and digitalised forms of credit cards via smartphones and smartwatches. However, this development of digitalisation also has negative effects, as it provides an excellent breeding ground for cybercrime.

3. Forms of cybercrime, with a special focus on money laundering

As technology advances, so does the variety of crime. Thanks to digitalisation, so-called cybercrime is now of major importance, and according to the literature, there are several generations of cybercrime. These include old crimes committed with the use of a computer, crimes committed via the Internet and real cybercrimes. (Wall, 2007) So you can see that most of the crimes are not entirely new, they have only changed in that they have moved to a new platform. In comparison, the new cybercrimes have been created using new technologies and depend on information networks. These platforms are ideal for committing crimes, as they provide users with almost complete anonymity (for example, in the case of cryptocurrencies), remove physical barriers, and make transactions easily accessible and fast. In the past, cybercrime required a high level of IT skills, but nowadays these interfaces are accessible to almost anyone, making anyone a perpetrator and a victim. (Dornfeld, 2019) The emergence of new technologies such as smart devices and artificial intelligence, as well as the spread of information networks, are leading to new and new ways of committing crimes. As a result, the range of offences punishable is also expanding. Since, as we have already seen, not only new offences are emerging as a result of digitalisation, but also new offences may be added to those already criminalised, this development poses significant challenges for legislators and law enforcement.

The term ‘cyberspace’ was first coined in the early 1980s by the author William Gibson to describe a global computer network connecting people (Gibson, 1982). In today’s literature, the term is used as a catch-all term to describe a range of offences that can be committed using information systems. The punishable conduct that is the subject of an information system is referred to as cybercrime in the narrower sense. The broader approach also includes traditional crimes committed using information systems. Examples include child pornography and money laundering. So, when we talk about cybercrime, we can think of new offences that can be committed using information systems, where the protected legal object is the information system or computer data itself. We can also include crimes which, thanks to technological progress, are easier to commit with the help of information systems. (Parti et al., 2017)

The roots of criminal action against money laundering can be traced back to 1986, when the First Anti-Money Laundering Act was passed in the United States of America. Later, the UN, the Council of Europe and the European Communities, and later the European Union, recognised the importance of the offence and began to give it a high priority. However, globalisation has brought the phenomenon to unprecedented proportions. Digitalisation and the development of technology have made cross-border transactions much easier, thus creating scope for money laundering in the digital space. As we have already seen, money laundering is always linked to a predicate offence, the aim being to conceal the origin of the illicit wealth derived from it. It is therefore a double latent crime. And thanks to the modern technologies already mentioned, it is even easier to separate the money from the source. The fact that identity can be easily concealed, that a person can have several accounts under several names, and that transactions can appear to outsiders to be between several different people, plays a huge role in this. It is also helpful for the perpetrators that while a traditional financial institution is bound by strict rules (the Pmt mentioned above), online banking services can be used under less strict conditions due to the lack of personal appearance and identification. (Tropina, 2014; Dornfeld 2019)

There are three different views on cyber money laundering. One sees it as an offshoot of cybercrime, another sees it as a new technique of money laundering, and a third sees it as a completely new phenomenon. It is often linked to cybercrime and online organised crime, but it goes well beyond that, as it also plays a role in laundering the proceeds of online or offline crime. (Dornfeld, 2019)

The purpose of money laundering in cyberspace is the same as in real space, i.e. an illegal financial transaction to achieve the purpose of verifying the origin of the criminal wealth. In the past, criminals often disguised the illicit assets as gifts or inheritances, but in virtual space this is no longer necessary (Nagy et al., 2018). Thanks to digital techniques, criminals can use a variety of methods to help them disguise the origin of the money.

The purpose of money laundering in cyberspace is the same as in real space, i.e. an illegal financial transaction to achieve an apparently legal justification for the origin of the criminal wealth. In the past, criminals often disguised the illicit assets as gifts or inheritances, but in virtual space this is no longer necessary (Nagy et al., 2018).

Cyber-money laundering is based on so-called electronic money, which has no physical form and can be perceived as a form of data stored on a computer. The lack of physical appearance makes it significantly easier to manipulate and to disguise its origin. The placement phase is also a higher risk factor, but while the appearance of large amounts of cash may raise questions, the chances of this happening with electronic money are lower.

One of the main trends in cybercrime is targeting online banking customers, so perpetrators need to use regulated financial intermediaries to launder assets. A common modus operandi may be to deposit the money in small instalments or transfer it to the appropriate accounts. And in the case of international transfers, they can create a chain that eventually becomes completely untraceable (Tropina, 2014). The cash flow also makes it increasingly easy for perpetrators to operate. Thanks to the digitalisation developments of domestic financial institutions, ATMs for cash payments are now available almost everywhere. These have only an occasional transaction limit, but no daily limit on the number or value of deposits. This allows large amounts to be deposited in a bank account within a short period of time. The use of such devices is becoming increasingly widespread, as they are not time-limited and deposits can be made at any time of the day, thus offering convenience to customers. However, this increased method of payment places a huge burden on financial institutions, as the increased number of transactions makes it even more difficult to detect suspicious transactions.

One of the main trends in cybercrime is targeting online banking customers, so perpetrators need to use regulated financial intermediaries to launder assets. A common modus operandi may be to deposit the money in small instalments or transfer it to the appropriate accounts. And in the case of international transfers, they can create a chain that eventually becomes completely untraceable (Tropina, 2014). The cash flow also makes it increasingly easy for perpetrators to operate. Thanks to the digitalisation developments of domestic financial institutions, ATMs for cash payments are now available almost everywhere. These have only an occasional transaction limit, but no daily limit on the number or value of deposits. This allows large amounts to be deposited in a bank account within a short period of time. The use of such devices is becoming increasingly widespread, as they are not time-limited and deposits can be made at any time of the day, thus offering convenience to customers. However, this increased method of payment places a huge burden on financial institutions, as the increased number of transactions makes it even more difficult to detect suspicious transactions.

Other common forms of cyber money laundering include money laundering using cryptocurrencies and money laundering by money couriers, which will be discussed in more detail below.

4. Features of cryptocurrencies

Cryptocurrencies, such as Bitcoin or Ethereum, are virtual currencies secured by cryptography and operating on blockchain networks independent of banks and authorities (Szalay, 2019). The emergence of blockchain technology has spread the use of these cryptocurrencies. Their advantage is that they are a system without intermediaries, meaning that users can transact directly between each other. This is called a peer-to-peer system. It is not backed by any country, it has no central bank backing, and it is based solely on a mutual agreement and trust between the users (Mezei, 2020).

The characteristics of cryptocurrencies may differ from one another, but there are common features. These include the decentralisation mentioned above, which prevents public authorities from obtaining information on cryptocurrency transfers by request, as these transfers do not fall under the jurisdiction of any public authority or company. If criminals use a centralised, supervised service, they should be prepared for the possibility that information about them may be passed on. In the case of decentralised cryptocurrencies, this is not a threat. As everyone is subject to the same rules, they can be sure of what data is stored by the blockchain for each transaction and that only and exclusively this stored data can be accessed by the authorities (Halász, 2019).

Another common feature of cryptocurrencies is the high degree of anonymity, as it is in the interest of the offenders to keep their identity hidden during and after the act. If we look at traditional financial transactions, we can see that the party carrying out the transaction is required to provide personal information. Even in this situation, the perpetrators can game the system, but this causes many difficulties. However, in the case of transactions with cryptocurrencies, in order to create a digital wallet, it is not necessary to provide personal data and a person can have a myriad of virtual addresses to which transfers can be directed. It should be noted, however, that although the persons behind each wallet carry out their transactions anonymously, the transfers themselves, their direction and their amount can be traced. This is why it can be considered as a pseudoanonim, since, once an address can be identified and its owner linked to it, all transactions received or initiated at that address can be traced back to a person (Möser, 2013).

The characteristic of cryptocurrencies is their easy accessibility, and the ease of access at any time through a wallet that can be created with a few clicks. Transfers can be initiated from anywhere at any time of the day, with only one condition: an internet connection. The transfers can be made as instant transfers, like those provided by traditional financial institutions, or can take a few minutes. For Bitcoin, this means 10 minutes. The transfer time for a domestic transfer is not very different from the transfer time provided by financial institutions, but for a transfer abroad there is a time difference, as it can take up to days for the funds to reach the target account.

Other common features include ease of ownership. As cryptocurrencies are effectively a series of characters, there are numerous ways to store them, which are difficult for authorities to detect (Halász, 2019).

Another attraction for criminals is that cryptocurrency can be obtained not only indirectly, through referrals by others, but also through so-called mining. This mining is a so-called distributed consensual system through which anyone can participate in the maintenance of crypto networks. In the case of earlier types of Proof of Work cryptocurrencies such as Bitcoin, mining is essential, but in the case of the newer Proof of Stake blockchain, mining is no longer required.

With Proof of Work blockchains, the chronological order of transactions is determined by mining, so it is not possible to change the previous mining data. For a transaction to be successful, it must be compressed into a block that conforms to strict rules. This is checked by the network's miners, who

enforce the rules. This is why Bitcoin networks are neutral, as no government authority is involved in the process. Transactions are validated by the miners, who produce new Bitcoins in the process.

In the course of mining, users discover new cryptocurrency units with a predefined and increasing difficulty and energy consumption. The miners who are considered the most successful add new blocks to the blockchain as they work. For this they are rewarded with Bitcoins. This used to happen regularly, as the process was not energy-intensive, but now no one has the computing power to create a new block on their own. To allow this to happen, users form communities, pool their capacity and then share the rewards in proportion to their contribution. Initially, the reward for creating 1 block was 50 Bitcoin, but this was reduced to 25 in 2012. This downward trend has continued, with a halving every four years. (*Hogyan működik a kriptovaluta bányászata.* https://kriptomat.io/hu/kriptovalutak/mi-a-kriptobanyaszat/, 2023. 07. 22.)

Money laundering through cryptocurrencies can be made even more attractive to the perpetrators by the fact that there is no uniform legal standard for them, and in most countries they are not regulated at all. These new virtual currencies have created challenges for legislators that have not yet been fully addressed. Given the cross-border emergence and use of cryptocurrencies, only uniform regulation can prevent the crimes they commit. However, this would be difficult to enforce and there are no general rules restricting cryptocurrencies at international or national level. However, it cannot be said that there are no legal standards at all. Attempts have been made to legally define cryptocurrencies in the European Union, most notably in Germany, but all Member States agree that they cannot be considered money in the absence of an issuer (Halász, 2019).

The first steps towards a coherent approach to cryptocurrencies were taken by Directive 2018/843 of the European Parliament and of the Council, known as the Fifth Anti-Money Laundering Directive. It requires a wider range of service providers to apply the AML/KYC requirements and encourages cryptocurrency holders to identify themselves.

The Directive states that the scope of Directive (EU) 2015/849 should be extended to providers of virtual currency and scriptural money exchange services and to depository wallet providers. In order to combat money laundering, public authorities should be able to monitor the use of virtual payment instruments through these service providers. As virtual payment instruments are anonymous, the Directive also draws attention to the fact that they can be used to increase the opportunities for criminals. However, it should also be noted that the extension of the scope of the Directive to include providers of virtual currency and scriptural money exchange services and to custodian wallet providers does not fully address the problems of anonymity of transactions carried out with virtual currencies, as the virtual currency environment will remain anonymous to a large extent, as users can carry out transactions without using such providers. In order to combat the risks associated with anonymity, it is necessary to allow national financial information units to collect the information necessary to associate the address of the virtual currency with the identity of the virtual currency holder.

The Directive also defines precisely what is meant by virtual payment instruments. It states: *"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;"* On this basis, it should not be confused with the concept of electronic money as defined in Directive 2009/110/EC, the comprehensive concept of money in Directive (EU) 2015/2366, and although cryptocurrencies are often used as a means of traditional payment, they have a much wider application. Such other uses include use as a medium of exchange, investment vehicle, store of value product and payment in online casinos. Directive 2018/843

aims to cover all possible uses. [Az Európai Parlament és a Tanács (EU) 2018/843 irányelve *a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról*]

The next major step in the fight against money laundering involving cryptocurrencies was the Commission Communication 2020/C 164/06. The Commission adopted a new package of proposals, which consisted of four legislative acts. The first of these is the creation of a new Regulation establishing an EU authority for the fight against money laundering and terrorist financing (Jacsó, 2022). The aim is to create a sixth anti-money laundering directive to replace Directive 2015/849. Of particular relevance to our study is the fourth legal act, which aims to revise the Money Transfers Regulation 2015/847 in order to monitor crypto-transfers. This is also important because (as we have already seen) only a small proportion of cryptoasset providers are subject to EU rules on combating money laundering and terrorist financing. By contrast, the new proposal would extend these rules to the entire crypto sector, thus obliging all providers to carry out appropriate customer due diligence. The review that will result from the package of proposals will ensure full traceability of crypto-transfers such as Bitcoin transactions. A further objective is to detect and prevent the use of such transactions for money laundering. In addition, they want to remove the anonymity that has been so attractive so far by banning the use of anonymous crypto wallets and calling for full application of EU rules on combating money laundering and terrorist financing by service providers and users. (Bizottság 2020/C 164/06 Közleménye)

Regulatory developments are underway, the status of which can be found in the press releases issued by the Council of the EU.

A provisional agreement on the transparency of cryptocurrency transfers has been reached, according to a statement published on 29 June 2022. The Council Presidency and a delegation from the Parliament have agreed to extend the rules on money transfers to cover part of the transactions with crypto assets. The provisional agreement was expected to provide the EU with a proportionate framework that would also comply with the highest international standards for exchanges, in particular the recommendations of the Financial Action Task Force (FATF). The new agreement requires that all data on the originator of the transaction must accompany the transfer of cryptoassets, regardless of the amount of cryptocurrency. Separate requirements will also be introduced for transactions between cryptoasset providers and independently managed wallets. With regard to data protection, the rules of the current GDPR regulation will not be tightened. The traceability of crypto-transfers will make it more difficult to circumvent sanctions. However, the service providers concerned will have to put in place appropriate internal procedures to mitigate the risk. A further important element of this interim agreement is that states must ensure that all cryptoasset providers are designated as obligated service providers in the future. (EU Tanácsa, 2022)

Regulation (EU) 2023/1113 of the European Parliament and of the Council on data accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 entered into force on 29 June 2023. The previous Regulation (EU) 2015/847 applied only to transfers of funds (banknotes and coins), scriptural money and electronic money as defined in Directive 2009/110/EC of the European Parliament and of the Council, and in order to comply with the revised FATF recommendations in 2019, it was necessary to introduce new legislation for virtual asset transfers in the EU. The EU legislator recognised that the flow of funds from illicit activities through wire transfers and virtual asset transfers could harm the integrity, stability and reputation of the financial sector and pose a threat to the EU internal market and international development [(EU) 2023/1113 rendelete, Preambulum 1–7]. The new regulation devotes a specific chapter to the obligations of crypto asset providers. It will specify the information that must accompany each cryptocurrency transaction, such as the name of the originator,

the shared ledger address, the name of the beneficiary, etc. A separate chapter will also cover the common measures to be applied by payment service providers and crypto service providers, which will be subject to guidelines to be issued by the European Banking Authority. (Az Európai Parlament és a Tanács 2023/1113 rendelete *a pénzátutalásokat és egyes kriptoeszköz-átruházásokat kísérő adatokról és az EU 2015/849 irányelv módosításáról*)

Other regulations currently in force include Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto instruments, amending Regulations (EU) 1093/2010 and 1095/2010 and Directives 2013/36/EU and 2019/1937/EU. The scope of the Regulation covers natural and legal persons and certain other undertakings that are engaged in issuing, offering to the public or admitting to trading, or providing services in relation to, cryptoassets in the European Union [Article 2(1)]. The Regulation defines cryptoasset as a digital representation of value or of a right that can be transferred and stored electronically using distributed ledger technology or similar technology [Article 3(1)]. This Regulation defines exactly which cryptoassets are covered by the Regulation, the requirements for their introduction to the market, the requirements for issuers and the protection of service providers' customers. Cryptoassets of the asset-based token type and the electronic money token type will be regulated separately. The conditions for the authorisation of service providers and their obligations are also detailed. Compliance with the rules on the prevention of money laundering and terrorist financing, such as the obligations imposed by Directive (EU) 2015/849 [Article 18(2)(g)] is of particular importance: Furthermore, one of the grounds for refusal of authorisation is where the business model of the applicant issuer could expose the issuer or the industry to a serious risk of money laundering and terrorist financing [Article 21(2)(e)]. There is a separate title on preventing market abuse of crypto-assets. (Az Európai Parlament és a Tanács 2023/1114 rendelete *a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról*)

5. The phenomenon of money mule

Offenders have developed a wide variety of methods to conceal the criminal assets derived from money laundering offences. Among these, the use of so-called money couriers has become one of the most popular methods, alongside the laundering of cryptocurrencies.

But who are money couriers?

A "money mule" is a person who voluntarily gives their details because they want to get easy money, as criminals often offer "quick, easy money" for participating in a fraud scheme with suitable offers. They are often aware that they are breaking the law, but in all cases they are aware of all the consequences. Criminals using money couriers give no real reason why this process is necessary.

The general role of 'money couriers' is either to open bank accounts themselves and then give the criminals access and full control, or the fraudsters open the accounts with their data. Both methods allow them to later commit various crimes, such as money laundering or terrorist financing.

Money muling, also known as counterfeiting, is a method of money laundering. Money muling is an activity carried out by money transmitters whereby money is accepted from a third party through a bank account or any other payment service and transferred to another (third) party. These "service providers" may take money in cash to send to someone else or convert it into cryptocurrencies to transfer it to another crypto wallet. In this way, the money transmitters receive a small portion of the transferred money in exchange for their service. The money is most often derived from crimes such as fraud, but can also come from drug or human trafficking activities. Money couriers willingly or unwittingly help

organised criminals to conceal their identity from the authorities, potentially making them accomplices in crimes committed to obtain the money transferred.

Money mules are usually recruited through social networks such as Snapchat, Facebook, Instagram or even dating sites, but also through fake recruitment websites and word of mouth. Labelled under an opaque job title, these offers advertise high financial rewards for working from home, for little work and limited effort, with no relevant experience or specific financial qualifications required. The tasks of the money couriers, who usually receive emails from their 'employers', are fairly straightforward:

- Open one or more bank accounts in their own name or in the name of a company they have set up;
- Receive the money in the bank account and transfer it to financial services, while keeping a portion as a commission.

According to Europol, the perpetrators are most likely to target newcomers to the country, the unemployed and students in financial difficulties. They are usually under 35 years old, but it has been found that organised crime groups have also targeted younger generations (12 to 21 years old). Even if these posts are detected and deleted by regulators, criminals can easily re-post fraudulent ads.

The competent authorities may consider the transfer of funds to third parties, usually belonging to organised criminal organisations, as aiding and abetting serious crime. Therefore, money couriers may put themselves at risk, even if they are unaware of the scheme as a whole. They can therefore continue to be prosecuted as accessories to laundering the proceeds of crime, face fines and/or imprisonment.

The FBI has also warned that any of the couriers could face criminal prosecution and jail time on charges including wire fraud, bank fraud, money laundering and aggravated identity theft. From a U.S. perspective, the federal agency adds that serving as a money smuggler can damage your personal credit score as well as your financial situation. In the UK, police indicate that the phenomenon of the money mule can have the following consequences:

- Closure of bank accounts used for money laundering activities;
- Difficulties in applying for loans or student loans;
- Difficulties in obtaining a telephone contract;
- A prison sentence of up to fourteen years. (https://www.idnow.io/glossary/money-mules/)

In the United States of America, the FBI is also particularly concerned with the phenomenon of money laundering. According to their definition, there are several types of money couriers. These are:

- Unaware money transmitters: in this case, individuals are unaware that they are part of a larger scheme. Often through an online dating programme or job offer, they are asked to use their existing personal bank account or open a new account in their real name to receive money from someone they have never met in person. In this case, usually the unsuspecting victim so 'hired' can keep some of the money transferred. In such cases, the money couriers are motivated by the prospect of a romantic relationship or confidence in the actual existence of a job offer.
- Conscious moneylenders: Individuals ignore obvious warning signs or deliberately act blindly to their money-changing activities. They may, for example, have been warned by bank employees that they are engaging in fraudulent activity, but this does not prevent them from continuing their activities. It is common for them to open an account in their real name with several banks. They may not initially know why the money is being moved, but they continue to communicate and participate. Their main motivation is financial gain or lack of recognition of their role.
- Associated money traffickers: individuals here are aware of their role from the outset, actively participating in the illeal processes. They open bank accounts on a regular basis to receive money from various individuals/businesses for criminal purposes. They also often advertise their services as money couriers, including what activities they offer and at what price. This may include

evaluating and/or rating other criminal actors on the speed and reliability of the money transmitter. They travel to different countries at the direction of their principals to open financial accounts or register companies. A frequent task is to recruit other money transmitters. Their motivation is mostly financial gain or loyalty to a known criminal group. (FBI. *Money Mules.* https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules)

6. Summary

In summary, the prevention of money laundering and terrorist financing has historically played an increasing role in government policy and the functioning of the economy, yet it was relatively late in the process, from 1986 onwards, that the relevant legal standards were established. However, it is clear that money laundering is an ever-changing offence. The health emergency of recent years, together with digitalisation and technological advances, are playing an increasingly important role in the management of money. In this environment, with increased transaction numbers and technological competition between financial institutions, it is becoming easier for criminals to legitimize the wealth derived from crime. So-called cyber money laundering has become common, where digital money is used to legalise assets through online platforms, and cryptocurrencies are increasingly associated with money laundering. The anonymity and decentralisation of traditional cryptocurrencies also play a major role in this. However, to address this, a package of proposals was put in place in 2021 to revise Directive 2015/8497 on data accompanying transfers of funds and to extend its scope to cryptocurrencies. This legislative process included an interim agreement in 2022 and an agreement in May 2023 on rules to ensure the traceability of crypto asset transfers. The two regulations adopted in May 2023, which set out detailed rules on the provision of data to accompany crypto-transfers and on crypto asset markets, are an important step in the fight against money laundering in the European Union and an important tool in the fight against money laundering. However, modern-day money launderers do not only operate effectively in cyberspace, but also continue to move money in physical form, often using couriers. We believe that the adoption by the EU legislator of the Commission's proposals in 2021 will further enhance the coherence of Member States' action against money laundering, which will contribute to more effective cooperation between competent authorities.

References

[1] Ambrus I. (2021). *Digitalizáció és büntetőjog*. Budapest: Wolters Kluwer Hungary.

[2] Jacsó J. (2019). A pénzmosás compliance hazai és európai dimenzióban a társadalmi innováció tükrében. *Miskolci Jogi Szemle*, 14, 2. különszám (1), pp. 394–412.

[3] 2017. évi LIII. törvény *a pénzmosás és a terrorizmus finanszírozása megakadályozásáról*. Preambulum.

[4] Jacsó, J. (2021). Straf- und Bußgreldrechtliche Verantwortung von Verbänden im Geldwaschestrafrecht. *European Integration Studies*, 17 (1), pp. 117–134. **https://doi.org/10.46941/2021.se1.117-134**

[5] Lentner Cs., Zéman Z. (2017). A pénzmosás egyes jogi és gazdasági összefüggései. *Miskolci Jogi Szemle*, 12 (1), pp. 19–32.

[6] Nagy A. (2020). Digitalizáció és mesterséges intelligencia a magyar igazságszolgáltatásban. *Miskolci Jogi Szemle*, 15 (1), pp. 19–32.

[7] Mezei K. (2019). A pénzintézetek ellen intézett kibertámadások büntetőjogi vonatkozásai. *Infokommunikáció és jog*, 1. 2019 (1), pp. 14–20.

[8] Gibson, W. (1984). *Neuromancer.* New York: Ace Books.

[9] Wall, S. S. (2007). *The transformation of crime in the information age*. Cambridge: Polity Press, pp. 44–48.

[10] Dornfeld L. (2019). Pénzmosás a kibertérben. In: Farkas, Dannecker, Jacsó (szerk.). *Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusai.* Budapest: Wolters Kluwer Hungary, pp. 451–461.

[11] Mezei K. (2020). A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam- és Jogtudomány*, 2020 (4), pp. 65–81.

[12] Parti K., Kiss T. (2017). Az informatikai bűnözés. In: Borbíró A., Gönczöl K., Kerezsi K., Lévay M. (szerk.). *Kriminológia.* Budapest: Wolters Kluwer Hungary, pp. 491–493.

[13] Mezei K. (2019). A kiberbűnözés szabályozási kihívásai a büntetőjogban. *Ügyészek Lapja*, 2019/4–5, 26, http://ugyeszeklapja.hu/?p=2592 (2023. 07. 31.)

[14] Tropina, T. (2014). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. *ERA Forum*, 2014 (1), p. 69, **https://doi.org/10.1007/s12027-014-0335-2**

[15] Nagy Z., Mezei K. (2018). Pénzmosás a kibertérben. *Infokommunikáció és Jog*, 2018 (1), pp. 26–31.

[16] Szalay G. (2019). A kriptovaluták nemzetközi szabályozási trendjei. *Jogtudományi Közlöny*, 2019 (3), 126–134.

[17] Halász V. (2019). A bűncselekményből származó vagyon nyomon követésének új kihívásai a kibertérben. In: Farkas, Dannecker, Jacsó (szerk.). *Az Európai Unió pénzügyi érdekei védelmének büntetőjogi aspektusai.* Budapest: Wolters Kluwer Hungary, pp. 433–443.

[18] Möser, M. (2013). *Anonymity of Bitcoin Transactions*. https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf (2023. 07. 21.)

[19] *Hogyan működik a kriptovaluta bányászata*. https://kriptomat.io/hu/kriptovalutak/mi-a-kripto banyaszat/ (2023. 07. 22.)

[20] Az Európai Parlament és a Tanács (EU) 2018/843 irányelve *a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról* OJ L 156, 19.6.2018, pp. 43–74.

[21] Jacsó J. (2022). A pénzmosás elleni küzdelemről szóló új javaslatcsomag – Különös tekintettel a Pénzmosás és Terrorizmusfinanszírozás Elleni Küzdelem Hatóságra. In: Koltay A., Gellér B. (szerk.). *Jó kormányzás és büntetőjog: Ünnepi tanulmányok Kis Norbert egyetemi tanár 50. születésnapjára*. Budapest: Ludovika Egyetemi Kiadó, pp. 307–319.

[22] Bizottság 2020/C 164/06 Közleménye OJ C 164, 13.5.2020, 21–33. **https://doi.org/10.1055/a-1211-3312**

[23] Az EU Tanácsa 2022. Sajtóközlemény. *A pénzmosás elleni küzdelem: ideiglenes megállapodás született a kriptoeszköz-átutalások átláthatóságáról.* Council of the EU Press HU 555/22 2022. 06. 29. https://www.consilium.europa.eu/hu/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/pdf (2023. 07. 22.)

[24] Az EU Tanácsa 2023. Sajtóközlemény. *A pénzmosás elleni küzdelem: a Tanács kriptoeszköz-átutalások visszakövethetőségét biztosító szabályokat fogadott el.* Council of the EU Press HU 321/23 2023. 05. 16. https://www.consilium.europa.eu/hu/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable/pdf (2023. 07. 22.)

[25] Az Európai Parlament és a Tanács 2023/1113 rendelete *a pénzátutalásokat és egyes kriptoeszköz-átruházásokat kísérő adatokról és az EU 2015/849 irányelv módosításáról* OJ L 150, 9.6.2023, pp. 1–39.

[26] Az Európai Parlament és a Tanács 2023/1114 rendelete *a kriptoeszközök piacairól, valamint az 1093/2010/EU és az 1095/2010/EU rendelet, továbbá a 2013/36/EU és az (EU) 2019/1937 irányelv módosításáról* OJ L 150, 9.6.2023, pp. 40–205.

[27] *Money Mules.* https://www.idnow.io/glossary/money-mules/ (2023. 07. 22.)

[28] FBI. *Money mules.* https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules (2023. 07. 22.)