DANUBE • 13(4) • pp. 256–268
DOI: 10.2478/danb-2022-0016

sciendo Danube

The New Hungarian Legislation on Money Laundering and the Current Challenges of Cryptocurrencies

István Ambrus[1], **Kitti Mezei**[2]

Abstract

Money laundering is one of the most important criminal offences today, perceived in the context of economic operation. Nevertheless, money laundering is a constantly changing phenomenon that is also influenced by the latest technological advancements. In this study, our aim is, after briefly outlining the phenomenon of money laundering, to review the new statutory definition(s) and those assessment criteria that may also be of significance for legal practice in this context from 2021 onwards in Hungary. Subsequently, we will describe the current challenges of cryptocurrencies regarding the new Hungarian and EU legislation on money laundering. The method we use is criminal law-dogmatic and retrospective analysis. The analysis concluded that the Hungarian legislator has significantly broadened the scope of money laundering, and a much wider spread of this offence is predicted for the future.

Keywords

Money Laundering, Cryptocurrencies, Hungarian Legislation, 5th Money Laundering Directive

I. Introduction

Money laundering (section 399–400 of the Act C of 2012 on the Criminal Code, hereinafter referred to as Criminal Code) is one of the most important criminal offences today, perceived in the context of economic operation (Gál and Tóth, 2004, p. 186). From the perspective of criminal law, this delict has been characterised by several specific features already in the past, according to which it was "out" of the scope both of the "ordinary" and of the so-called ancillary offences (or offences of criminal connections). It is out of the scope of the former one as it assumes the existence of a predicate offence and of the latter

[1] Eötvös Loránd University, Egyetem square 1–3, 1053 Budapest, Hungary, and Centre for Social Sciences, Institute for Legal Studies, Tóth Kálmán street 4., 1097 Budapest, Hungary. E-mail: ambrus.istvan@ajk.elte.hu.
[2] Centre for Social Sciences, Institute for Legal Studies, Tóth Kálmán street 4., 1097 Budapest, Hungary, and Budapest University of Technology and Economics, Magyar tudósok körútja 2., 1117 Budapest, Hungary. E-mail: mezei.kitti@tk.hu.

one because the mentioned predicate offence does not necessarily need to be committed by guilt or proven in its entirety, or it may even be the case that the predicate offence and money laundering are committed by the same person.

However, the fact that – partly to comply with EU Directive 2018/1673 – section 53 of Act XLIII of 2020 on the amendment of the Act on Criminal Procedure and other related acts, *had introduced entirely new provisions in relation to the criminal offence with effect from 1 January 2021*, makes the issue of money laundering particularly relevant. Under this heading of the study, after briefly outlining the phenomenon of money laundering, we will review the new statutory definition(s) and those assessment criteria that may also be of significance for legal practice in this context from 2021 onwards in Hungary. As researchers of economic criminal law, the motivation for our analysis was the fact that the definition of money laundering in Hungary has been completely changed as of 2021, and a comprehensive overview of this new regulation has not yet been published in the international literature. In view of this, we feel that the preparation of this analysis is particularly timely and topical. Subsequently, we will describe the current challenges of cryptocurrencies regarding the legislation on money laundering.

II. Money Laundering in General

Money laundering is a very complex concept. The understanding and handling of which challenges the legislators, the authorities and the service providers covered by the legal provisions relating to preventing money laundering. The general concept of money laundering may be defined as concealing the origin of the benefit derived from the illegal activity. The persons and institutions participating in money laundering aim to achieve by the execution of different, often purposefully difficult operations that the money, otherwise acquired illegally, appears in the outside world, especially to the authorities, already as a legal income and can be used for further activities, whether legal or illegal. Thus, money laundering as a phenomenon assumes at least one, but typically several activities usually involving organised crimes, e.g., criminal offences involving drugs, prostitution, human trafficking, illegal gambling, corruption or damage to public funds, which generate significant amounts of illicit income. The greater the income from illegal activity, the greater the chance that the amount of money thus acquired also attracts the attention of the authorities, who make by virtue of their powers the necessary measures to prosecute the offenders and deprive them of the assets they have illegally obtained. Besides, eventually, the need will arise in the offenders of the crimes to secure their money thus acquired and to use it for different but already legal economic activities as well. However, circumventing the authorities, disguising and securing the proceeds of illegal activities and injecting them into the legal economy is no easy task. It requires a high level of organisation, cross-border and complex financial and legal structures. These structures are not realised and executed by the perpetrators themselves but by involving and/or using those special experts (for example, bankers, lawyers, accountants, money changers, etc.) who have the expertise and background to help offenders find the ideal way to disguise the origin of money.

Nevertheless, money laundering is a constantly changing phenomenon that is also influenced by the latest technological advancements. Nowadays, economic and living conditions became complex due to technical development. Technical barriers or national borders no longer hinder financial flows; actors in the financial sector also tend to operate internationally. The complexity of their activities and the high number of transactions they carry out also make detection difficult for the authorities. For that very reason, the fight against money laundering places a particularly heavy burden on the service providers and public authorities involved. An effective fight against money laundering can be achieved only on an international level, through coordinated legislation and enforcement and a high level of cooperation between public authorities.

Of course, at the same time, money laundering is also a criminal offence; that is, countries such as our country also punish money laundering with the utmost rigour by means of criminal law. However, it does not mean that the criminal statutory definition of money laundering corresponds to its everyday concept, which is shortly defined by the Preamble of the Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing (hereinafter referred to as Act on Money Laundering) as laundering the money or other financial means derived from the commission of criminal offences through activities exposed to the threat of money laundering. However, despite this declaration, the Act on Money Laundering, *de iure* uses the definition of the Criminal Code on money laundering as section 3(26) of the Act on Money Laundering states that for the purposes of the act conducts defined in section 399–400 of the Criminal Code may be regarded as money laundering.

III. The New Statutory Definition of Money Laundering

The Criminal Code regulates the crime of money laundering – also in a somewhat specific way – under an entirely independent and separate chapter. Already in the past, Chapter XL defined very complex acts falling under the criminal offence of money laundering, which is concerned by significant amendments from 1 January 2021 onwards can be found in Sections 339–400 of the Hungarian Criminal Code. Due to the length of the new legislation, it will not be cited in its entirety, but the analysis will refer to the main changes.

Of course, besides these significant modifications, several similarities can be shown as well. Thus, money laundering by negligence is still punishable, in connection to which the ground terminating punishability is also maintained in the act. As before, it does not constitute a specific offence committed by a person who has the necessary personal qualifications, for example, if committed by a public officer, etc.

Each type of the offence shall be analysed one by one, given their significant differences. However, it is common in all types that the legal subject of money laundering is basically the public interest related to repel organised crime and to the social need that assets derived from criminal offences should not remain in the offender's hands.

The material object of the *first basic type* is the asset derived from criminal activity. With the phrase criminal activity, the law intends to express that money laundering may be established even in the absence of culpability of the predicate offence (e.g., the perpetrator

of the predicate offence has a mental disorder), and the scope of assets is wider than that of the property set out in the previous statutory definition, thus, including not only physically existing objects, assets but also rights and claims. This version is a material offence, a so-called *open statutory definition* according to the ministerial reasoning of the amending Act. The conduct of concealing or disguising involves more than the passive retention of assets of the criminal origin or the proper use. The result of these conducts is that the assets lose their original characteristics and appear to the outside world as if the incriminated assets were not derived from a criminal offence. Thus, the result can be defined in the quality that the origin of assets becomes concealed or disguised. These two conducts and the result based on them cover different contents. Concealing means that the criminal origin of assets becomes a secret to the outside world. In contrast, disguising contains an additional element, as it requires a disguising title, that is, the criminal origin of assets disappears, and it gives the appearance of a legal origin. The first basic type is not purposeful on the subjective side; thus, it can even be committed with indirect intent.
The *second basic type* is a *sui generis preparatory* variant of the first. The partial acts are, in essence, separately punishable acts connected to the state before completion, which intentionally seek the result included in the first basic type. It is an important regulatory principal identified under Directive 2018/1673 that the criminalisation of these partial acts is primarily given by the fact that their overarching aim is to cover criminal assets. This justifies the fact that the second basic type can also be established in relation to assets resulting from the own criminal act of the perpetrator without prejudice to the *ne bis in idem* principle.
The third basic type is an *accessory after the fact type* of money laundering. In this regard, under Directive 2018/1673, any intentional provision of assistance to evade the legal consequences under criminal law shall be punished. The criminal legal consequence for assets derived from criminal activity is confiscation or possibly the bringing of civil law claims relating to assets also subject to confiscation. These substantive legal measures are indirectly aimed at the final deprivation of the assets of criminal origin. Confiscation or asset recovery includes all legal consequences that are applicable under criminal law in relation to assets derived from criminal offences, hence, avoiding the legal consequences related to assets may consist in avoiding the application of these two institutions.
By creating the *fourth basic type*, the legislator incorporated handling stolen goods constituting an individual crime for the last 140 years into money laundering, thus, from 2021, the above-mentioned traditional crime against property is no longer part of substantive law, we can only refer to it as a historical category or as the present type of money laundering. However, it is a significant change that handling stolen goods may only be committed in relation to a property derived from ten exhaustively listed crimes (or for non-community goods removed from customs control or products removed from excise taxation) under section 379 of the Criminal Code in force until 31 December 2020, but in contrast, the predicate offence of this, handling stolen goods type of money laundering can be any punishable act. The scope of conducts also became wider, thus, besides acquisition, concealment, and contribution to alienation, several further activities (e.g., use, transformation, etc.) also constitute this type of money laundering.

Money laundering will constitute a basic type in all intentional cases if it is involving assets worth up to 50 million forints (116,342 GBP). It is a significant change that money laundering is simply punishable by imprisonment up to 5 years instead of 1 to 5 years, so the general minimum of imprisonment, three months, shall be applicable. Parallel to the statutory definition, the legislator also amended section 33(4) of the Criminal Code, which enabled to impose a so-called *alternative penalty/sanction* (by reviving the solution known from the Act IV of 1978) for all criminal offences where the lower limit of the range of punishment does not reach one year. Accordingly, it applies also to money laundering, and therefore if it involves a value of 50 million forints or less, the court may decide, even in the absence of any mitigating circumstances, to impose confinement, community service, fine, etc. instead of imprisonment, or – if none of the prohibitions of co-application applies – it can impose more than one as well. In such cases – and even in the qualified case under section 399(6) of the Criminal Code punishable by imprisonment of 2 to 8 years – District Courts shall have jurisdiction at first instance under the amended section 20(1)(20) of Act XC of 2017 on Criminal Procedure. Only the most serious money laundering offences punishable by imprisonment of 5 to 10 years fall under the jurisdiction of Regional Courts as courts of the first instance [section 399(7) of the Criminal Code].

It shall also be highlighted that the legislator created a *regulatory offence* type of money laundering, namely if money laundering involves a maximum amount of 50,000 forints [section 462(2)(g) of the Criminal Code].

Today, not only the agreement on joint commission – such as one of the specified cases of preparation – shall be punishable by the law, but also each type of preparation, for example ensuring the necessary conditions for commission, invitation, undertaking, etc.

The legislator narrowed and simplified the scope of qualifying circumstances as only acts committed for a value above 50 million forints, or a value between 5 and 50 million forints are involved, if the activity is performed in a business-like manner or as a service provider defined in the Act on Money Laundering, or as the officer or employee thereof in conjunction with the activity of the service provider, or as a public officer. Henceforth, an attorney may only be liable for the basic and not for the qualified case.

The *negligent* conduct shall remain punishable by section 400(1) of the Criminal Code, as we already referred to it, but assets constitute the material object even here. Here, the scope of qualifying circumstances also changed. However, the ground terminating punishability remained, which is the privilege of the person reporting the negligent money laundering.

Money laundering, as already cited, constitutes a concurrence of offences with the preliminary act essentially. Therefore, *"laundering of own money"* shall be separately punishable (BH 2014. 7.). Section 399(9) of the Criminal Code creates an exemption to this, according to which the instigator and the abettor may not be punished in relation to the third and fourth basic type of the crime, if he commits the money laundering for assets originating from a punishable act committed by him. Naturally, it follows, by *argumentum a contrario*, from the legislation that the perpetrator of the preliminary act shall already be liable for money laundering related to his own punishable act. The cited special ground precluding punishability dogmatically constitutes, in essence, a criminal unity, where a real concurrence of offences should be established in relation to money laundering. Therefore,

the general rule governing offences of criminal connections is restored, according to which the person involved in the predicate offence shall not be punishable for money laundering in relation thereto. Hence, the latter constitutes an ancillary (unpunished) offence.
It can also be pointed out that the Criminal Code continues to punish, as a misdemeanour, the failure to comply with the statutory reporting obligation concerning the prevention of money laundering and terrorist financing [section 400(1) of the Criminal Code]. The rule prescribes the reporting obligation in section 30 of the Act on Money Laundering. Thus, the Criminal Code refers to another act, the Act on Money Laundering (framework disposition), and so the provisions of the Act on Money Laundering give the substance to the criminal statutory definition. The scope of the Act on Money Laundering, containing the special obligations related to the prevention of money laundering (and of terrorist financing), is narrower than that of the Criminal Code as only those exhaustively listed service providers are covered by the act whose field of activity is the most vulnerable in terms of money laundering (terrorist financing).
Under section 1 of the Act on Money Laundering, as in force from 10 January 2020, these service providers are credit institutions; financial services providers; institutions for occupational retirement provision; voluntary mutual insurance funds; entities taking in and delivering international post money orders; entities engaged in activities related to real property transactions; entities engaged in auditor activities; entities operating casinos or card rooms or organising betting not qualifying as remote gambling, remote gambling or online casino games, etc., established in or having a branch or place of business in Hungary.

IV. Cryptocurrencies and Money Laundering

Money laundering challenges legislators, especially in the age of virtual currencies, which provide an increasingly sophisticated, harder to follow way for laundering the illegally obtained proceeds. The use of cryptocurrencies involves money laundering and terrorist financing risks due to *decentralised infrastructure* and *pseudo-anonym transactions*.
Cryptocurrencies laundering schemes are similar in their intents to traditional money laundering schemes (De Sanctis, 2019, p. 74). Transactions may be used to account for legal business operations, but also for illegal activities. Converting the proceeds of crime into cryptocurrencies then forwarding them to different addresses provides the possibility of laundering them. All stages of money laundering may be implemented, in a way similar to fiat money, also when using virtual currencies. Cryptocurrencies facilitate placement because a significant number of wallets can be created anonymously, either free of charge or at low cost and risk. Layering (hiding) is carried out by multiple transfers between different wallets and/or by exchanging different cryptocurrencies and fiat money, or by a cryptocurrency-to-cryptocurrency exchange (Poskriakov, Chiriaeva and Cavin, 2019).
In relation to the conversion of cryptocurrencies, various services are available that make it difficult to track transactions. These include:

* The already mentioned *virtual currency exchange platforms* help exchange between cryptocurrencies and legal tender (for example, Kraken, Coinbase, Bitstamp). These are such providers of online crypto exchange markets or crypto exchange services

that operate in an open and transparent way (have, for example, customer identification, detailed terms of use).

- *Mixing* and *tumbling services* available on the darknet either divide a common address containing a more significant amount into smaller ones, or vice versa combine several smaller amounts under one common address. Their aim is to hide the link between the original source and the new cryptocurrency address by conducting multi-step transactions. These service providers often advertise themselves by deleting the transaction history within a short period of time.
- *ShapesShift* provides exchange between different cryptocurrencies, which is subject to registration.
- By using the *atomic swap*, exchange into another cryptocurrency is possible through a smart contract without the intervention of a third party (see more Ramalho and Matos, 2021, pp. 487–506).

In the light of all the above, since 2013, undertakings providing services related to cryptocurrencies in the United States have been treated essentially in the same way as other undertakings providing financial services. However, until now, providers of crypto exchange services have had no obligation to identify suspicious activities at the EU level. Consequently, criminals – or even terrorist groups – could transfer money into the EU financial system, or within virtual currency systems that offer a high degree of anonymity, making money transfers untraceable.

On a proposal submitted by the Commission, on 30 May 2018, the European Parliament and the Council adopted the *5th anti-money laundering Directive*, which has the novelty of defining the concept of virtual currency for the first time. According to Article 3(19) it *"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"*.

Moreover, virtual currencies should not be confused with electronic money, with the larger concept of "funds", nor with a monetary value stored on instruments exempted as specified in points (k) and (l) of Article 3 of *Directive (EU) 2015/2366*, nor with in-games currencies, that can be used exclusively within a specific game environment. Although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos. The objective of the 5th anti-money laundering Directive is to cover all the potential uses of virtual currencies.

It is a significant step that its scope was extended to include additional obliged entities engaged in *exchange services between virtual currencies and fiat currencies*, as well as *custodian wallet providers*. The latter is defined in Article 3(19) of the 5th anti-money laundering Directive as: *"an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies"*.

This category includes only service providers which provide their services as an online hot wallet and those which do not guarantee this by means of dedicated hardware or software developed for users (Covolo, 2019, p. 15).

In essence, the new legislation is based on the fact that the system of virtual currencies is decentralised since there is no central supervisory body and therefore no one to turn to for information related to transactions. However, with the assistance of service providers covered by the 5th anti-money laundering Directive, the cryptographic keys – in other words, the addresses and private keys – belong to registered customers who can thereby be identified, and providers can ensure additional information on transactions to the authorities in cases where the users make use of such services.

The aim is to enable the competent authorities, through obliged entities, to monitor the use of virtual currencies for the purposes of anti-money laundering and countering the financing of terrorism. The 5th anti-money laundering Directive imposes the *know your customer (KYC)* requirement on obliged entities which, through a defined customer due diligence process, facilitates to mitigate the risks of money laundering and terrorist financing. The obliged entities shall collect as much data as possible about their customers in order to be aware of their activities, the nature of their business relationships and their financial habits. The know-your-customer process and transaction monitoring together can ensure the system's transparency. In the case of providers of exchange and custodian wallet services, the following measures are relevant: identifying the customer when opening a user account; record-keeping and preparing reports; reporting suspicious activities; setting up an internal regulatory system (for example, internal rules, training, employing a *compliance officer*, etc.) For instance, the Financial Action Task Force (FATF) has accepted standards that require countries to assess and mitigate their risks associated with virtual asset financial activities and providers; license or register providers and subject them to supervision or monitoring by competent national authorities (See more FATF, 2021).

According to Article 47(1) of the 5th anti-money laundering Directive, Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered. However, providers engaged in exchange services between virtual currencies, crypto exchange markets and trading platforms are not within its scope (Covolo, 2019, p. 14–15 and see more Haffke, Fromberger and Zimmermann, 2020, pp. 125–138).

It should be noted that this will not entirely address the issue of anonymity attached to virtual currency transactions because users can also transact without such providers as they do not necessarily have to be converted into legal tender. To combat the risks related to anonymity, national Financial Intelligence Units should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed.

Member States had to transpose the 5th anti-money laundering Directive into national law by 10 January 2020. To discharge this duty, Act CXIX of 2019 on the amendment of Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing

and of other related acts were adopted, which amended Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing (Act on Money Laundering) with effect from 10 January 2020. As a result, Hungarian law now also includes the concept of virtual currencies and a new list of providers has been brought within the scope of the Act on Money Laundering, thus, under the supervision of the Hungarian Financial Intelligence Unit.

Under section 65(1) of the Act on Money Laundering, the providers are required to draw up internal rules to perform tasks covered by statutory obligations. If the activity covered by the Act on Money Laundering is started after the entry into force of the amendment, or the activity (providers engaged in exchange services between virtual currencies and fiat currencies, or virtual currencies, as well as custodian wallet providers) is brought within the scope of the Act by the amendment, the provider shall prepare and submit for approval to the Hungarian Financial Intelligence Unit an internal rule within 45 days as of it starting its activity according to section 65(9) of the Act on Money Laundering.

In addition, section 3(47) of the Act on Money Laundering lays down the concept of virtual currency as follows: *"a digital representation of value that is not issued or guaranteed by a central bank or a public authority; it does not possess a legal status of legal tender; it can be stored electronically, is accepted as a means of exchange, and thus can particularly, be transferred and traded electronically"*. The list of obliged service providers and the personal scope of the act has been extended in line with the EU legislation.

The Commission shall draw up a report on its implementation and submit it to the European Parliament and to the Council by 11 January 2022 and every three years thereafter. The first report, to be published by 11 January 2022, shall be accompanied, if necessary, by appropriate legislative proposals, including, where appropriate, with respect to virtual currencies, empowerments to set up and maintain a central database registering users' identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users, and to improve cooperation between Asset Recovery Offices of the Member States and a risk-based application of the measures referred to in point (b) of Article 20.

It is worth mentioning that on 20 July 2021, the Commission presented its proposal for the 6th Directive on money laundering and terrorist financing, which will replace the existing Directive 2015/849. It aims to harmonise EU law through the introduction of 22 "predicate offences", including new offences of cybercrime and environmental crime. Due to the requirement to file suspicious activity reports, cryptocurrency service providers should ensure their staff are trained to identify the risks associated with potential criminal behaviour. The 6th anti-money laundering directive has also extended liability to include legal persons, as well as individuals. This means that corporate entities may be held liable for money laundering offences and will not be in a position to shift the blame onto rogue employees.

In the following, we will examine the Hungarian legislation on money laundering regarding cryptocurrencies. First, we deal with the material object of money laundering which is, according to the provisions in force in 2020, property derived from criminal activity. The term *"property"* is not specifically defined in the Criminal Code or in the Act V of 2013

on the Civil Code (hereinafter referred to as Civil Code), but in the interpretative provision of the *Strasbourg Convention* in Article 1(b) as follows: *"'property' includes property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title to, or interest in such property."* This definition is directly enforceable in the application of the statutory definition of money laundering. Section 5:14(1) of the Civil Code merely states that physical objects that can be taken into possession can be objects of ownership. Under the interpretative provision of section 402(1) of the Criminal Code, for the purposes of sections 399 to 400, the property also means any instrument embodying a pecuniary right, including a dematerialised security, that confers the right of disposal over the certified pecuniary value or right in and of itself or, with respect to dematerialised securities, to the beneficiary of the securities account.
The 2021 new legislation makes significant changes in the statutory definition of money laundering, its material object is amended and supplemented in content. According to the reasoning, the conceptual framework of property under the previous legislation became restrictive in view of the new types of assets that have recently emerged, such as the various forms of electronic data for payment. We have previously drawn attention to the fact that these can be included in the conceptual frameworks of criminal law, as they can be subject to confiscation under the rules of the general part. However, there was a contradiction between the fact that certain types of assets could be subject to confiscation but could not constitute the material object of money laundering. To resolve this, it became necessary to draw up flexible legislation that is equally suitable to deal with the new types of assets within the scope of the statutory definition of money laundering. As stated in the reasoning, amending the material object of money laundering to assets creates sufficiently flexible conditions for the fight against crimes committed through the new types of assets. Using this definition also ensures compliance with international and EU requirements. Conferring the right of disposal over assets appears as a new conduct.
The second issue is related to the conduct, namely, in the case of *self-laundering and dynamic money laundering*, performing a financial activity or utilising a financial service for the purpose of concealing, disguising the origin of the property which is defined by the interpretative provisions contained in section 402(2) of the act. It is also important as offenders frequently use various providers of exchange and wallet services through which they carry out transactions or exchange cryptocurrencies. The question may arise, whether the activity of these providers constitutes a *financial service or a supplementary financial service*. The current legislation does not yet define it. An amendment to the background legislation (Act on Credit Institutions and Financial Enterprises) is needed to make this happen, but this is not the task of criminal law. This points out that not only cryptocurrency itself should be handled by legislation, but also activities related to its use, its forms of use, for example, the operation of payment systems, the operation of trading platforms, mining, storage, or crypto-based derivatives. Currently, these activities cannot be fully integrated into the systems of terms used in our laws on financial matters. Therefore, they need to be amended or supplemented.

By involving virtual currencies, such traditional and well-known money laundering methods as the *money mule phenomenon* can take on a new character. In this case, the perpetrators, pretending to be the representatives of virtual currency exchange platforms, offer employment contracts, whereby the "job" of the requested party would be to receive significant amounts from the money changer on his personal account and then withdraw it in cash or transfer it to payment accounts defined by the *"employer"* – in return for a commission, of course. The person who accepts such an offer also becomes involved in the commission of the negligent version of money laundering.

V. Conclusion

As a summary, it can be concluded that the Hungarian legislator introduced fundamentally modern changes which are expected to meet EU requirements by way of the new legislation on money laundering in force from 2021. By incorporating the offence of handling stolen goods into money laundering, the number of money laundering cases is expected to increase in the criminal statistic, as acts previously classified as handling stolen goods will also be automatically added to the data of money laundering cases. To demonstrate this with numbers: according to the ENYÜBS [Unified System of Criminal Statistics of Investigative Authorities and of Public Prosecution] database 357 cases of handling stolen goods, while 188 cases of money laundering were detected in the country in 2019. In the next year, in 2020, 422 cases of handling stolen goods and 308 cases of money laundering came to the attention of the authorities. Thus, a significant increase can be observed in the statistical numbers of money laundering cases itself (previously only 20 to 30 cases were detected per year) and if the data of handling stolen goods are also added to this from 2021 onwards, around 1000 offences could be easily registered per year. However, in the light of the newest statistical numbers, our previous prediction was a bit pessimist: in 2021, finally, 358 cases of money laundering and 263 cases of handling stolen goods have been registered, probably not inseparable from the COVID-19 pandemic (Ambrus, 2021, pp. 470–471).

A considerable part of these crimes will be trivial ones since an act, previously constituting a simple type of handling stolen goods involving 60 to 80 thousand forints (139–186 GBP) will also constitute money laundering. The legislator correctly assessed the situation by providing for imposing alternative sanctions and the jurisdiction of the district courts at first instance, whereas imprisonment can be avoided in many cases and regional courts do not become overwhelmed due to the rising number of money laundering cases.

As regards the first basic type of the offence, with an open statutory definition, it can be highlighted that in view of this conceptual classification, this version of the offence may also be committed by omission by the person having a special obligation (for example, under an employment relationship) to prevent the result. However, this circumstance should encourage anti-money laundering professionals to be even more prudent and cautious, such as the complete criminalisation of the stage of preparation.

The consistent application of that basic requirement for the statutory definition, according to which assets of criminal origin cannot remain in the offender's hands, hence, they should be more widely deprived of him by using the full range of criminal law measures also be accepted.

Finally, it must be mentioned that the greatest challenge in detecting crimes committed with the use of cryptocurrencies, is that transactions cannot be linked to any particular individual, because identification or authentication is not required for the transfers. Thanks to *decentralisation*, virtual payment systems have no central supervisory body. In other words, the competent authorities have nowhere to turn for the necessary information in a criminal procedure. For instance, in the case of financial institutions where, upon a simple inquiry with the bank, it is easy to trace financial flows and identify the individuals sending and receiving the money. The EU recognised that the use of cryptocurrencies and various exchange and wallet services poses money laundering and terrorist financing risks. Therefore, the scope of the 5th anti-money laundering Directive (*Directive 2018/843 of the European Parliament and of the Council*) has also been extended to include these service providers who shall also comply with the more stringent anti-money laundering or "know your customer" rules. However, the new legislation does not apply to providers of crypto-to-crypto exchange services and crypto exchange markets and trading platforms. Furthermore, it is also possible to carry out operations relating to cryptocurrencies without using such services. As a novelty, the Directive defined the term of virtual currencies for the first time.

When examining the Hungarian legislation, it can be concluded that the domestic statutory definition of money laundering, in particular, shows the deficiency concerning this offence as its material object, the term of *property* derived from a criminal offence, cannot be correctly applied to cryptocurrencies. The new legislation in force since 2021 provides a solution for this problem, introducing the term of asset into the statutory definition of money laundering due to international legislation. In addition, legislation should cover cryptocurrencies and the activities relating to them, for example, the activities of the providers of exchange, investment, and wallet services within the framework of financial services or supplementary financial services, which requires an amendment to the background legislation. Thus, that is not primarily the task of criminal law.

Acknowledgements

The research was supported by the Ministry of Innovation and Technology NRDI Office within the framework of the FK_21 Young Researcher Excellence Program (138965) and the Artificial Intelligence National Laboratory Program.

References

Ambrus, I. (2021). The COVID-19 pandemic and Hungarian substantive criminal law. *Zeitschrift für Internationale Strafrechtsdogmatik*, 16(7–8), 462–471.

Covolo, V. (2019). The EU Response to Criminal Misuse of Cryptocurrencies: The young, already outdated 5th Anti-Money Laundering Directive. *University of Luxembourg Law Working Paper Series* No. 2019-015 p 15.

De Sanctis, F. M. (2019). *Technology-Enhanced Methods of Money Laundering: Internet as Criminal Means*. Springer.

Financial Action Task Force (FATF) (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.

Gál, I. L., Tóth, M. (2004). The Fight against Money Laundering in Hungary. *Journal of Money Laundering Control*, 8(2), 186–192.

Haffke, L., Fromberger, M. Zimmermann, P. (2020). Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them. *Journal of Banking Regulation*, 21(2), 125–138.

Poskriakov, F., Chiriaeva, M., Cavin, C. (2019). Cryptocurrency compliance and risks: a European KYC/AMLP perspective. In Josias Dewey (ed.): *Blockchain & Cryptocurrency Regulation 2019*, Global Legal Group.

Ramalho, D. S., Matos, N. I. (2021). What we do in the (digital) shadows: anti-money laundering regulation and a bitcoin-mixing criminal problem. *ERA Forum 2021*, 22, 487–506.

U.S. Department of Justice. (2018). *Report of the Attorney General's Cyber Digital Task Force*. Washington.