CRIMINAL LAW ASPECTS OF DIGITAL ASSETS – CONTEMPORARY CHALLENGES

Jovana Banović, PhD[1]
Faculty of Security Studies, University of Belgrade, Serbia

Introduction

By adopting Law on Digital Assets (LoDA, Official Gazette RS, 153/2020) in 2020., Serbia became one of the first countries in the world that regulates realm of digital assets. Among others, the enactment of the aforementioned law aimed to prevent the abuse of digital assets and their criminal misuse. A few years prior, Law on the Prevention of Money Laundering and the Financing of Terrorism (LoPMLFT, Official Gazette RS, 113/2017, 91/2019, and 153/2020) also stipulated virtual currencies in accordance with the aforementioned law. Additionally, it is essential to emphasize significance of the newest European Union Regulation 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCA). This regulation raises critical questions about digital assets and associated risks and is expected to pave the way for future legislation governing the digital landscape within the European Union.

Theoretically speaking, we are currently facing an atypical situation in Serbia. According to fundamental principles, Criminal law should possess an *ultima ratio* character, encompassing subsidiary application and the protection of fragmentary types of goods. The notion of fragmentarity is pertinent to the subject of this article, as it implies that Criminal law does not create the values it protects, but rather identifies them in other fields of law. In a broader sense, we are currently witnessing a sort of *vice versa* scenario – digital and virtual assets are initially encountered within the context of Criminal law, concerning abuse or money laundering, before being subsequently integrated into the conceptual framework that defines the terms associated with these concepts. This article's focal point will be on offences linked to Digital assets, as defined by the Law on Digital Assets (LoDA), and the potential application of existing provisions within the Criminal Code of Serbia to address the aforementioned legal issues.

Design/Methods/Approach

The research paper comprises an introduction, three distinct chapters, and a conclusion. The first chapter provides a brief elucidation of the normative framework, encompassing pertinent provisions from the LoDA, LoPMLFT, Criminal Code of Serbia (CC, Official Gazette RS, 5/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, and 35/2019) and MiCA regulation. The emphasis lies on the overarching provisions relevant to digital assets, particularly the legislative foundation underpinning the enactment of LoDA (Official Gazette RS, 153/2020) and its interplay with CC and LoPMLFT (Official Gazette RS, 113/2017, 91/2019, and 153/2020), accompanied by an overview of appropriate regulations set forth by MiCA. The second chapter delves into an analysis of two offences outlined in LoDA (Official Gazette RS, 153/2020). From a criminal law perspective, this exploration

1 jovanabanovicc@gmail.com

encompasses the penal aspects of insider trading and market manipulation. The third segment of the article addresses queries concerning existing provisions within the CC that could potentially pertain to digital assets, encompassing criminal offences against property, computer data security, economic interests, and related matters.

The scientific method employed here primarily incorporates a doctrinal approach, utilizing content analysis, the dogmatic method, and a conceptual approach. Given that this Article is founded on legal provisions, a normative analysis has been employed to assess the existing state of digital assets concerning crimes involving cryptocurrency usage, while also addressing the challenges posed within the context of contemporary challenges.

The Normative Framework and Certain Fundamental Principles

Before presenting the main provisions of the aforementioned laws, we will establish some fundamental terms. Firstly, the terms 'digital assets' and 'virtual assets' will be used interchangeably, as LoDA (Official Gazette RS, 153/2020) treats them as synonyms. In fact, the Law explicitly provides the definition as follows: "digital assets, or virtual assets, means…" (Art. 2, Par. 1, pt. 1). Undoubtedly, both digital and virtual assets encompass broader categories than virtual or cryptocurrencies (for example, see Art. 2, Par 1, pt. 2 of LoDA; The Report – The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets, 2022: 4). This examination will also delve into relevant questions about virtual currencies, as they represent the most common form of digital assets.

LoDA (Official Gazette RS, 153/2020) serves as the foundation for considering the main subject of this Article. This law came into force on June 29th, 2021. Article 2, par. 1, pt. 1 and 2 of the Law define "digital assets, or virtual assets' as 'a digital representation of value that can be digitally bought, sold, exchanged, or transferred and used as a means of exchange or for investment purposes. Digital assets do not include digital representations of fiat currencies and other financial assets governed by different laws, unless otherwise specified by this Law." Similarly, the Law specifies that "virtual currency means a type of digital asset that is not issued or guaranteed by a central bank or public authority, is not necessarily tied to legal tender, and lacks the legal status of money or currency. However, it is accepted by natural or legal persons as a medium of exchange and can be bought, sold, exchanged, transferred, and electronically stored." With these definitions in mind, several conclusions can be drawn. Digital assets represent specific property rights or property values in digital format, often symbolized by tokens. This parallels the logic of symbols representing property rights or values in physical form, such as banknotes or coins. Additionally, the concepts of 'digital,' 'virtual,' and 'crypto' can be discerned. What these terms share is their non-physical existence. These attributes capture the nature or essence of digital assets that include and crypto currencies: 'digital' highlights their basis in computer technology, 'virtual' denotes their operation in the online and virtual realm, and 'crypto' signifies a certain level of secrecy (Schueffel, Groeneweg & Baldegger, 2019: 11, 14; Fairfield, 2017: 172-174).

While LoDA (Official Gazette RS, 153/2020) provides the foundation for comprehending the realm of digital assets, it is essential to underscore the significance of LoPMLFT (Official Gazette RS, 113/2017, 91/2019, and 153/2020) within the Serbian justice system. This marked the initial legal enactment through which 'virtual currencies' were regulated. Although virtual currencies were first *mentioned* in the same-titled law (LoPMLFT, Official Gazette RS, 113/2017), their more comprehensively regulated definition was missing.[2] This was achieved more detailed through amendments to LoPMLFT as docu-

2 This was done in a provision (Art. 4, par. 1, pt. 16 LoPMLFT) that stated: "Entities engaging in the provision of services

mented in Official Gazette RS, 91/2019. Subsequent amendments of LoPMLFT in Official Gazette RS, 153/2020 'harmonized' these definitions in relation to LoDA (Official Gazette RS, 153/2020). Thus far, we can confirm that the Law on Digital Assets has adopted the virtual currency definition as stipulated in LoPMLFT, Official Gazette RS, 91/2019. This stands as the current state of our legislation. Now, let's take a step back.

The main reason for legislative intervention in the context of virtual currencies within LoPMLFT was to prevent offenders and criminal groups from abusing virtual currencies in their illegal activities. This intervention aligns with the obligations of harmonization with the European Union *Acquis*, a collection of Community (*Communautaire)* rules contained in legal acts and court decisions. This is an important obligation for both EU member states and candidate countries. Conceptually, the legal foundation for the initial regulation of virtual currencies in Serbia is based on aligning Serbian law with Directive (EU) 2018/843 of The European Parliament and of The Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Directive 2018). *Inter alia,* the Directive's preamble explains that the anonymity of virtual currencies can lead to their potential misuse for criminal purposes. To counter these risks, national Financial Intelligence Units (FIUs) should be able to obtain information that links virtual currency addresses to the identities of their owners. Chronologically, this legislative situation is interesting from the perspective of the fundamental principles of Criminal law, particularly in terms of fragmentarity as part of the *ultima ratio* character of Criminal law. Virtual assets initially enter the realm of Criminal law due to issues of abuse, money laundering, and terrorist financing, before being formally defined within legislative frameworks. This unique situation underscores the contemporary challenges that the law must address, even if it requires exceptions from traditional rules. For instance, the decentralization and anonymity inherent in digital currencies contribute to this evolving legal landscape (Czarnecki, 2017: 287). Similar dilemmas can arise in defining movables according to Art. 112 Par. 16 of the Criminal Code. While 'digital assets' can find acceptance within criminal law, it cannot be entirely equated with the terms used in civil and property law (Damnjanović, 2022: 80).

It should be kept in mind that this type of process is complex and continually challenged. The recent Financial Action Task Force (FATF) Report serves as evidence of this. Reporting on the implementation of Recommendation 15, the report underscores that "some jurisdictions have introduced regulations standards on Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs), but global implementation is relatively poor and compliance remains behind most other financial sectors. Based on 98 FATF mutual evaluation and follow-up reports since the standards on VAs and VASPs were adopted, three quarters of jurisdictions (75%; 73 of 98) are only partially or not compliant with the FATF's requirements" (FATF, 2023: 2). This data holds significance, especially when considering that Serbia, unlike many jurisdictions with low global compliance, has adopted a substantial number of standards pertaining to virtual assets.

Finally, MiCA establishes the most detailed regulations for digital assets at the European Union level. From the perspective of Criminal Law, a few points warrant emphasis. Firstly, it prohibits the behavior that can undermine user confidence in crypto-asset markets and their integrity. Specifically, under Title VI – Prevention and Prohibition of Market Abuse Involving Crypto-Assets, the following provisions can be found: Article 89 stipulates the Prohibition of insider dealing, Article 90 prohibits the Unlawful disclosure of inside information, and Article 91 prohibits market manipulation. Moreover,

for the purchase, sale, or transfer of virtual currencies, or the exchange of these currencies for money or other assets, through internet platforms, physical devices, or other means, or entities that mediate in the provision of these services." However, almost complete harmonization followed, as will be explained further below.

administrative penalties and other measures are proscribed for these infringements, without prejudice to potential criminal penalties and the supervisory and investigative powers of competent authorities (Art. 111, MiCA). Considering that the Serbian legislator sanctions these illicit activities through penal law provisions, it is intriguing to examine the second part of Art. 111, MiCA. It allows Member States to opt not to establish rules for administrative penalties if the infringements mentioned in the first subparagraph are already subject to criminal penalties in their national law by 30 June 2024. Given that LoDA (Official Gazette RS, 153/2020) criminalizes the aforementioned conducts, it can be inferred that Serbian law has taken a step further even before the EU officially did, prescribing more stringent forms of punishment than what MiCA requires (criminal, not solely administrative). However, there are differing viewpoints regarding the justification of criminal law protection concerning insider dealing, especially considering its *ultima ratio* nature (more about the new trends in EU Criminal law: Faure & Leger, 2015: 389, 426-427). Nevertheless, contemporary criminal law must align with and judiciously assess modern trends (Aryamov, Grachova, Chuchaev & Malikov, 2019: 2).

Criminal Law Protection of Digital Assets – Articles 140 and 141 of LoDA

LoDA (Official Gazette RS, No. 153/2020) introduces two relatively new criminal offences. We say "relatively" because Serbian law already has the same offences in nature. Articles 140 and 141 of LoDA prohibit illicit use of inside information and market manipulation referred to digital assets. However, Capital Market Law – CML (Official Gazette RS, 129/2021) contains two almost identical criminal offences: Prohibition of market manipulation (Art. 402) and Use, disclosure and recommendation of insider information (Art. 403) (see more: Jovanović, V. Radović & M. Radović, 2020: 607-615). Regarding the subject of the Article, a brief analysis of digital assets-related crimes will be given below.

Article 140 of LoDA – Insider Dealing

The offence consists of a basic form, two qualified forms and the most serious form of this offence. Additionally, there is a specific paragraph stipulating a punishment for attempting the basic form of the crime, as it would not be punishable under general rules. According to the Law, the offence is committed when the perpetrator uses inside information with the intention of acquiring financial benefits for themselves or for other persons, or causes damage to other persons. Illicit use of inside information that is done with intention of earning financial benefits or causing damage is prohibited when it is alternatively perpetrated as following: directly or indirectly during the acquisition, alienation or attempts to acquire or alienate for own account or the account of another holder the digital assets to which such information relates, or by disclosing and making available inside information to any other person, or by recommending or inducing another person, based on inside information, to acquire or alienate digital assets to which such inside information relates. For this form of the offence, the penalty is imprisonment for up to one year, including a fine.

The object of protection is inside information or more precisely – its misuse. Domestic law protects various types of secrets (see: Bodrožić & Milošević, 2022). Inside information, being privileged, is a component of that system. The LoDA (Official Gazette RS,153/2020) provides definition of inside information in Article 39. This refers to information about specific facts that are non-public and relate directly and indirectly to one or more issuers or one or more types of digital assets, which, if made public, would be likely to have a significant effect on the price of such digital assets. Subsequent paragraphs elaborate on what constitutes a 'significant effect,' the characteristics that information must possess to qualify as insider information, and the implications for individuals responsible for carrying

out orders related to digital assets. With regard to the aforementioned provision, several basic characteristics of this type of privileged information can be identified. Firstly, it must pertain to a specific fact concerning the issuer or digital asset. Secondly, it must not have been published. Lastly, the information should be of financial significance to a prudent investor. Intention is established as a subjective element of the offence, indicating that the relevant degree of guilt is direct intention.

The first qualified form occurs when the acquisition of financial benefits or the caused damages exceed the amount of RSD 1,500,000 (Art. 140, par. 2 of LoDA). The second qualified form arises when a person gains possession of inside information in the following ways: through membership in the management or supervisory bodies of the issuer, having a stake in the issuer's capital, accessing information obtained through normal employment, profession, or duties, or as a result of criminal offences committed. Both qualified forms require intent as a subjective element, and the perpetrator is subject to punishment by a fine or imprisonment of up to three years. In contrast to the basic form of the offence, which is committed by the secondary insider, the second qualified form should be committed by the primary insider. Due to their duty of loyalty and specific status as members or stakeholders, the penalty is more stringent (Radisavljević, 2023: 308; for further insight into specific duties and status-related crimes, refer to: Banović & Mihailović, 2021: 128-133). The most severe form of the offence is linked to this form of crime (Art. 140, par. 3 of LoDA) and arises when the acquisition of financial benefits or caused damages to other persons exceed the amount of RSD 1,500,000. The prescribed penalty is imprisonment for a duration of six months to five years, along with a fine.

Article 141 of LoDA – Market Manipulation

This offence exists in both a basic and a qualified form. The act of perpetration involves engaging in market manipulation to gain financial benefits, either for oneself or another person, or causing damage to others. Manipulation inherently carries a negative connotation, although not all forms of manipulation are illegal. Moreover, manipulation can be defined as "sophisticated, skillful handling or management of something, and also the creation of business tricks" (Vujaklija, 2009: 567). LoDA (Official Gazette RS, 153/2020) provides a comprehensive definition of market manipulation in Article 49. In summary, this definition covers: false or misleading signals or information regarding the supply, demand, or price of digital assets; maintaining the price of one or more digital assets at an abnormal or artificial level in connection with transactions or orders; engaging in fictitious actions or any other form of deception and contrivance; disseminating knowingly or potentially false or misleading information; transmitting such information, and more. If we consider the complete definition from the aforementioned Article 49 (along with the subsequent Article 50 that prohibits manipulation), we can comprehend unlawful manipulation as actions that contravene fair market competition rules, influencing the supply or demand of digital assets with the intent to gain financial benefits or cause damages. Such actions create a 'manipulative market' (in a negative sense) that operates outside the genuine laws of supply and demand. These actions erode the foundation of sound market competition (Watters, 2023: 5).

For the basic form of the offence, the offender shall be punished if they engage in the following actions, alternately: concluding transactions or issuing orders to trade that provide, or are likely to provide, false signals about the supply, demand, or price of digital assets, or where the price of one or more digital assets is artificially maintained at an abnormal level through collaboration (the first scenario); concluding transactions or issuing orders to trade that involve fictitious actions or any other form of deception or contrivance (the second scenario); disseminating information through the media, including the internet, or through any other means, that provides or is likely to provide false or misleading

signals about digital assets, when the disseminator knew or ought to have known that the information was false or misleading (the third scenario). In relation to the usage of the terms 'signals' or 'information' as elements of the crime, it is essential to mention certain debates in the literature (Radisavljević, 2023: 309). Additionally, the reach of the internet amplifies the opportunities for market manipulation (Swan, 2022: 196), as well as the commission of various criminal offences in general (Banović, 2019: 358-359). As for the subjective element, intent is required, despite the part of the incrimination using the construction 'ought to have known,' which is akin to the criteria of negligence, but can also suggest *dolus eventualis*, not solely *dolus directus*. It is important to underscore that punishment exclusively for intentional offences is justified from both a penal policy standpoint and a procedural perspective, as the occurrence of damage or benefit to a specific recipient facilitates evidence examination (Watters, 2023: 12). The prescribed penalties for this offense are imprisonment of six months to five years and a fine. Unlike the previous offence (Art. 140 of LoDA), where the special paragraph prescribing punishment for attempts is justified, in this case, attempted actions would be penalized according to Article 30 of CC (Official Gazette RS, 5/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, and 35/2019), and therefore, no specific paragraph is needed. In any case, the offence is deemed complete upon obtaining a benefit or causing damage.

The qualified form arises when the previously explained actions have caused a significant disruption in the digital assets market. The term 'significant disruption' represents the consequence of the offence and is punishable in accordance with the legal construction of liability for graver consequence (Article 27 of CC). In simpler terms, it is enough to consequence be attributed to the offender's negligence. However, if there are no other offences that could cause 'a significant disruption in the digital assets market', even intention due to the more severe consequence is conceivable. On the surface, this situation seems real, considering that digital assets are specifically protected by the penal provisions of the Law on Digital Assets. Nevertheless, in the context of the theory of causality (and the potential ingenuity and creativity of offenders), numerous actions beyond the elements of a specific crime could lead to a significant disruption. The question arises – should all of these actions be considered as suitable acts of perpetration according to the norms of Criminal Law? The only prescribed criminal sentence for this form is imprisonment for three to eight years. A fine is not specified in this form, but it could be imposed based on the general provisions of fines. If a criminal offence is committed for gain, a fine may be applied as a supplementary penalty even when not explicitly stipulated by law. However, it is worth considering that this omission might also indicate a legislative oversight in explicitly including the option of imposing a fine.

Digital Assets and Certain Provisions of the Criminal Code

Digital assets operate within the market, further implying the potential for substantial value exchange. These characteristics create opportunities for potential illicit activities across a range of protected objects. Initially, virtual assets faced criticism due to their potential involvement in criminal activities such as narcotics dealing, terrorism, tax evasion, money laundering, fraud, and more (Stabile, Prior & Hinkes, 2020: 298, 315; Watters, 2023: 4). The above-mentioned offences encompass crimes that could be perceived as violations of certain 'traditional' criminal law norms.

First and foremost, the Criminal Code of Serbia provides broad definitions of certain important terms in the context of digital assets, such as movables, computer data, computer program, and property gain. These definitions pertain to the objects of actions. Article 112, paragraph 16 of the Criminal Code stipulates that *movables* also include any produced or collected energy for emitting light, heat or

movement, telephone pulse, and computer data and computer program. In paragraphs 17 and 19, the Law further defines *computer data* as any representation of facts, information, or concepts in a form suitable for processing in a computer system, including an appropriate computer program necessary for the functioning of the computer system, and additionally, a *computer program* which is a regulated assembly of orders serving to control computer operation, as well as to solve a specific task by means of a computer. Lastly, the definition of *property gain* (given in Article 112, par. 36 of the Criminal Code) encompasses goods of any kind, tangible or intangible, movable or immovable, or the estimates and invaluable documents in any form that proves right or interest in relation to such well. Property is considered income or other benefit that originates, directly or indirectly, from criminal offence, as well in which it is converted or with which it is merged. It seems that these definitions are precise, comprehensive, and applicable in the context of digital assets.

Starting from the premise that digital assets constitute a category of property, it is natural to begin review with criminal offences against property. Offences that would come to the forefront will be: Theft (Art. 203 CC) and Aggravated Larceny (Art. 204 CC). Among the contentious issues, for example, these offences can raise the question of attempted and completed crime. Besides that, Embezzlement (Art. 207 CC) can also be considered. Furthermore, Extortion (Art. 214 CC) and Blackmail (Art. 215 CC) can also be taken into account. Having in mind that Fraud (Art. 208 CC) is classical property-crime, it can lead the problem of relation to Computer Fraud in the context of specious joinder offences by principle of specialty. Considering the fact that digital assets primarily require the use of technology, it will likely involve Computer Fraud. Particularly based on the provisions of Law on the Organisation and Competences of Government Authorities Combating Cyber Crime (LOCGACCC, Official Gazette RS, 61/2005, 104/2009 10/2023, 10/2023) that stipulated cybercrime for the purposes of this law. It shall mean committing criminal offences where computers, computer systems, computer data and products thereof in hard or electronic form appear as the objects or the means of committing a criminal offence (Art. 2 LOCGACCC). However, we cannot exclude the fact that digital assets can be defined as property, even in the sense of traditional crimes. By now, it is difficult to take clear stance without appropriate judicial praxis and "real matter". In this context, Swan (2022: 182) explains difference between "online" and "offline" crimes where the latter involve demanding money transfers. In any case, it is important to clarify what exactly constitutes the object of action or which interests are predominantly protected. Undoubtedly, the previously presented legal definitions help in that regard (both from LoDA and CC). Also, it is true that some traditional crimes can easily get certain digital shape (Swan, 2022: 196).[3]

The second group of offences that can be related to digital assets and their virtual character is – security of computer data. Especially, the following crimes: Creating and Introducing of Computer Viruses (Art. 300 CC), Computer Fraud (Art. 301 CC), Unauthorised Access to Computer, Computer Network or Electronic Data Processing (Art. 302 CC), Unauthorised Use of Computer of Computer Network (Art. 304 CC) and Creating, Obtaining and Providing another Person with Means for the Committing Criminal Offences against the Security of Computer Data Article (Art. 304a CC). It is compelling to make a parallel with ransomware misuse in the context of offence from the Article 300 of CC and Extortion and Blackmail from the articles 214 and 215 of CC. Ransomware attacks have been causing significant concern for computer systems, but also for security in general and also acting "online". Moreover, even European legislation is being shaped, considering that the field of digital as-

3 An interesting case involves the theft of electricity in the monumental home of a Serbian officer from the period of the First and Second World Wars. Namely, equipment for so-called cryptocurrency mining was connected to the low-voltage network through a meter that had been previously deregistered and was not in operation. "Za ilegalno rudarenje kriptovaluta u Dražinom spomen-domu potrošili 55.000 kW/h" (2021), https://n1info.rs/vesti/za-ilegalno-rudarenje-kriptovaluta-u-drazinom-spomen-domu-potrosili-55-000-kw/, Accessed on August 28, 2023.

sets is an area that offers many possibilities, but at the same time entails substantial risks (Mihailović *et al.*, 2022: 141-144). Given that they involve various objects of protection, these criminal offences would be considered in relation to joinder of offences (Putnik, Milošević & Cvetković, 2022: 329, 336-337; Swan, 2022: 182). *Modus operandi* can be viewed as follow: hackers attack commercial computer systems and blackmailed or extorted them looking for the financial gain. In order to regain access to their networks, companies (mostly the large ones) opt for payment because it costs them less than reputational risks, fines due to inadequate system protection, and especially - data loss (Swan, 2022: 193). Consequences of these actions are not naïve. They raise important questions that can rightly be considered as the leading challenges of the modern era. Thus, Lambert (2022: 21-23, 383) recognizes the importance of crypto currencies and data protection.

From the group of offences against economic interests, it is worth to mention Abuse of Trust in Conducting Business Activity (Art. 224a CC). That could be situation when service provider causes damage to the user by managing digital assets based on contractual relation. After that, probably the most indicative virtual assets-related offence is Money laundering from the Article 245 of Criminal Code. In this regard, some issues are touched before. At this point, specific questions will be underlined. Given that cryptocurrencies are characterized by anonymity, establishing guilt as a subjective element can be linked to greater difficulties. Especially in accordance to specific negligence form of this offence (Vuković, 2019: 134; Delić, 2021: 261). Furthermore, tax aspects related to digital assets have been addressed within the Serbian legislative framework (Milojević Kolarević, 2021). This is why Tax Avoidance (Art. 225 CC) can also be examined in relation to these objects of action.

Findings/Orginality/Value

Through the previous analyses, certain findings will be presented below. It can be concluded that Serbia has a solid foundation for the regulation of digital assets. In addition to the Law on Digital Assets, which constitutes the primary regulation in the realm of virtual assets, the protection of these assets can also be ensured in accordance with the Law on the Prevention of Money Laundering and the Financing of Terrorism, and, of course, the Criminal Code. The first of the aforementioned laws is significant for addressing fundamental issues such as definitions, supervision, various procedures, and, finally, the criminal law aspect stipulated in Articles 140 and 141, which outline two offences. The second law is important because it has introduced the topic of virtual assets for the first time. Specifically, the main reason for legislative intervention in the context of virtual assets within this law was to prevent offenders and criminal groups from exploiting virtual currencies in their illicit activities. The third law contains the fundamental principles of criminal law and represents an integral part of this analysis.

Theoretically, keeping in mind the fundamental principles of criminal law, it can be concluded that fragmentarity (which means that criminal law does not create values it protects, but rather finds them in other fields of law) as a part of the *ultima ratio* principle confirms that we are currently witnessing a certain *vice versa* example – that digital/virtual assets first appear in the context of criminal law abuse, and only afterward in the conceptual framework for defining the terms of those institutes and concepts. Furthermore, insider dealing and market manipulation are prohibited under Articles 140 and 141 of the Law on Digital Assets as new offences in secondary criminal legislation. However, these crimes are relatively new, considering that the Capital Market Law already criminalizes similar offences. The primary difference lies in the object of protection. Moreover, digital assets can be examined in relation to some 'traditional' crimes. This presents an additional reason for considering offences

proscribed by the Criminal Code of Serbia. Offences against property, security of computer data, and economic interests are identified as representative for analysis. Regarding the definitions of movables, computer data, computer programs, and property gain given in Article 112 of the Criminal Code, it can be concluded that the above-analyzed offences can be taken into account in the context of virtual assets. Furthermore, the recently adopted EU Regulation 2023/1114 of 31 May 2023 on markets in crypto-assets (MiCA) is worthy of mention, especially considering that the Serbian Law on Digital Assets is generally aligned with it even before MiCA comes into force within the EU territory. It is important to emphasize that harmonization with European Union legal documents is an important obligation for both EU member states and candidate countries.

Finally, the digital landscape certainly introduces a new and fruitful dimension to various areas of law. It raises numerous questions that can challenge traditional norms, particularly within branches of public law like Criminal law. Its norms exhibit a moderate resistance to change, but this does not imply that even this field of law should not keep up with new trends. Consequently, the existence of regulation in this realm is beneficial. While it is true that this regulation can be improved, especially considering that life is often more creative than the law itself, it remains essential. From the perspective of Criminal law, however, there is no a specific practice for evaluating the effectiveness of prescribed norms. Proper enforcement serves as a strong indicator when examining penal provisions. This applies not only to offences related to digital assets, but also to general provisions (*e.g.,* seizure and confiscation of virtual assets). Overall, this holds significance for the future development of what can be termed 'Digital Criminal Law'.

References

Aryamov, A., Grachova, V., Chuchaev, I. & Malikov, V. (2019). Digital Asset as an object legal regulation. *Ekonomika,* 65(2), 1–11. DOI: 10.5937/ekonomika1902001A

Banović, J. (2019). Javno podsticanje na izvršenje terorističkih dela (čl. 391A KZ): između slobode pojedinca i bezbednog društva. In: Đ. Ignjatović (Ed.), *Kaznena reakcija u Srbiji: tematska monografija* (deo 9, pp. 349–364), Beograd, Srbija: Univerzitet u Beogradu – Pravni fakultet.

Banović, J. & Mihailović, J. (2021). Direktor kao odgovorno lice – pojedini kompanijskopravni i krivičnopravni aspekti. *Godišnjak Fakulteta bezbednosti,* 1, 121–142. DOI: 10.5937/fb_godisnjak0-33325

Bodrožić, I. & Milošević, M. (2023). Secret as an object of criminal law protection in the Republic of Serbia. *XII International Scientific Conference "Archibald Reiss Days", Thematic Conference Proceedings of International Significance,* 12, 93–111.

Capital Market Law (CML), Official Gazette RS, No. 129/2021.

Criminal Code of Serbia (CC), Official Gazette RS, No. 5/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, and 35/2019.

Czarnecki, J. (2017). Digital Currencies and the Anti-money Laundering/Counter-terrorism Financing Regulations in the EU: Imaginary Risk or Real Challenge? In: K. Ligeti and M. Simonato (Eds.), *Chasing Criminal Money Challenges and Perspectives on Asset Recovery in the EU* (pp. 287–304), Oxford and Portland, Oregon: Hart Publishing.

Damnjanović, N. (2022). Pravna priroda kriptovaluta. *Harmonius,* 11, 71–96.

Delić, N. (2021). *Krivično pravo – posebni deo.* Beograd: Univerzitet u Beogradu - Pravni fakultet.

Directive (EU) 2018/843 of The European Parliament and of The Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

Fairfield, J. A. T. (2017). *Owned – Property, Privacy, and the New Digital Serfdom*. Cambridge: Cambridge University Press.

FATF (2023). Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, Downloaded July 1, 2023 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtualassets-vasps-2023.html .

Faure, M. G. & Leger, C. (2015). The Directive on Criminal Sanctions for Market Abuse: A Move Towards Harmonizing Inside Trading Criminal Law at the EU Level? *Brooklyn Journal of Corporate, Financial & Commercial Law*, 9(2), 387–427.

Jovanović, N., Radović, V. & Radović, M. (2020). *Kompanijsko pravo – Pravo privrednih društava.* Beograd: Pravni fakultet Univerziteta u Beogradu.

Lambert, P. (2022). *Gringras: The Laws of the Internet* (6th ed). London, New York, Dublin: Bloomsbury Professional.

Law on Digital Assets (LoDA), Official Gazette RS, No. 153/2020.

Law on the Organisation and Competences of Government Authorities Combating Cyber Crime (LOCGACCC), Official Gazette RS, No. 61/2005, 104/2009 10/2023,10/2023).

Law on the Prevention of Money Laundering and the Financing of Terrorism (LoPMLFT), Official Gazette RS, No. 113/2017, 91/2019, and 153/2020.

Mihailović, J. & Terzić Danilović, I. (2022): Pružaoci usluga povezanih s virtuelnim valutama – pojedini statusnopravni aspekti. *Pravo i privreda,* 1, 138–160. DOI: 10.55836/PiP_22107A

Milojević Kolarević, M. (2021). Poreski tretman digitalne imovine u Republici Srbiji. *Finansije*, 1-6, 46–74.

Putnik, N., Milošević, M. & Cvetković, V. N. (2022). Rensomver kao pretnja bezbednosti- društveni i krivičnopravni aspekti. *Sociološki pregled*, LVI (1), 328–353. DOI: 10.5937/socpreg56-36845 .

Radisavljević, I. (2023). Krivičnopravna zaštita digitalne imovine. In: Đ. Ignjatović (Ed.), *Kaznena reakcija u Srbiji: tematska monografija* (deo 13, pp. 302–314), Beograd, Srbija: Univerzitet u Beogradu – Pravni fakultet.

Regulation 2023/1114 of the European Parliament and of the Council (MiCA) of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

Schueffel, P., Groeneweg, N. & Baldegger, R. (2019). *The Crypto Encyclopedia - Coins, Tokens and Digital Assets from A to Z*. Bern: Growth Publisher.

Stabile, D. T., Prior, K. A. & Hinkes, A. M. (2020). *Digital Assets and Blockchain Technology – US Law and Regulation.* Cheltenham, UK•Northampton, MA, USA: Edward Elgar Publishing.

Swan, E. J. (2022). *Internet Law – A Concise Guide to Regulation Around the World.* The Netherlands: Wolters Kluwer.

U.S. Department of Justice (2022) The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role Of Law Enforcement In Detecting, Investigating, And Prosecut-

ing Criminal Activity Related To Digital Assets, Downloaded July 1, 2023 https://www.justice.gov/ag/page/file/1535236/download .

Vujaklija, M. (2009). *Rečnik stranih reči i izraza* (4. izdanje). Beograd: Prosveta.

Vuković, I. (2019). O izvesnim nedoumicama u pogledu krivičnopravne zaštite od pranja novca. *Crimen*, 2, 122-143. DOI: 10.5937/crimen1902122V

Watters, C. (2023). When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment. *Laws*, 12 (33), 1–16. DOI: 10.3390/ laws12020033

"Za ilegalno rudarenje kriptovaluta u Dražinom spomen-domu potrošili 55.000 kW/h" (2021), https://n1info.rs/vesti/za-ilegalno-rudarenje-kriptovaluta-u-drazinom-spomen-domu-potrosili-55-000-kw/, Accessed on August 28, 2023.