DOI: https://doi.org/10.30525/2256-0742/2023-9-4-134-147

METAVERSE: MODEL CRIMINAL CODE

Oleksii Kostenko[1], Dmytro Zhuravlov[2], Oleksii Dniprov[3], Oksana Korotiuk[4]

Abstract. The Scientific and Technical Revolution 5.0 and WEB 3.0 technologies create conditions for the renovation of various forms of social relations with the use of virtual and augmented reality technologies in the metaverse. According to the proposed theory, the legal regulation of social relations in the metaverse requires the development of a comprehensive electronic jurisdiction based on the latest basic legislation. The formation of legal regulation of the metaverse is a prerequisite for the need to form an electronic jurisdiction of the metaverse, which will include sectoral Metaverse Codes. The metaverse, as the electronic society of the future, does not yet have clear legal boundaries, and the task of scholars is to predict and outline with sufficient certainty the future contours of legal authority for virtual environments. Today, discussions in the scientific community about the feasibility and necessity of legal regulation of the metaverse often revolve around several key issues. First, there is the question of what legal framework should be applied in the metaverse and how conflicts between different legal systems should be resolved. Second, there is a debate about whether current regulatory bodies in the physical world have the capacity to effectively regulate the metaverse through existing laws and regulations. Third, there is the question of how to deal with offences committed in the virtual environment, and whether they should be dealt with under existing tort or criminal law, or whether a separate cross-border electronic jurisdiction should be created. The regulation of social relations in the metaverse should focus on one central goal: to clearly define the status of electronic entities, subjects and objects, to establish their rights, duties and responsibilities, and to define the different types of relations between virtual entities, subjects and objects within a given metaverse, as well as between different metaverses within an electronic jurisdiction and in a cross-border context. An essential component of the Metaverse Electronic Jurisdiction is a Metaverse Model Criminal Code that will outline the norms and offences applicable to analogue, hybrid and electronic jurisdictions. This code will define the types of socially harmful acts or crimes and the corresponding criminal penalties that will be applied within the metaverse. The formation of the electronic jurisdiction of the metaverse and the development of a Metaverse Model Criminal Code is a current scientific and legal issue.

Key words: metaverse, metaverse electronic jurisdiction, Metaverse Criminal Code, avatar, electronic personality, electronic humanoid, identification data, blockchain, AI, cryptocurrency, virtual objects, ownership of virtual objects, intellectual property, cybercrime, virtual crime, legal regulation of the metaverse.

JEL Classification: K24, K40

1. Introduction

The need for legal regulation of the metaverse is closely related to the need to formulate a theory and model of electronic jurisdiction for the metaverse, which will include industry-specific Metaverse Codes. By recognising e-jurisdiction and e-justice as important components of social relations in the Metaverse, the grounds for developing a comprehensive e-jurisdiction based on new legislation are seen.

The metaverse space creates the possibility to create and use avatars, electronic humanoids (personalities), other objects or subjects with or without special status.

[1] State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine", Ukraine *(corresponding author)*
E-mail: antizuk@gmail.com
ORCID: https://orcid.org/0000-0002-2131-0281
[2] Office of the President of Ukraine, Ukraine
E-mail: ndz0909@gmail.com
ORCID: https://orcid.org/0000-0002-2205-6828
[3] Office of the President of Ukraine, Ukraine
E-mail: osdniprov@gmail.com
ORCID: https://orcid.org/0000-0002-7157-9748
[4] State Tax University, Ukraine
E-mail: ovk@korotyuk.com
ORCID: https://orcid.org/0000-0003-0081-3901

The virtual identities of an individual may be fundamentally different from the main identification image registered on the current platform, but they will be more independent, have their own image and personality, form their own social relations, etc., forming a multi-vector identity system in the metaverse that can establish electronic social relations with other virtual objects. These relations, based on the essence of humanity, will not always be positive, and therefore it is necessary to develop rules of conduct and legal norms that will prevent destructive influence, the violation of which will result in the use of various measures of state coercion.

2. General Approaches to the Legal Regulation of Metaverse

The technological revolution 5.0 has given rise to the metaverse era, which is today shaping new social relations and confronting existing legal systems with the challenge of "broken windows" and "creative destruction" (Ma Changshan, 2018). The new challenges posed by metaverse technologies require constant innovation and improvement of national legal doctrines and international law to address new legal issues.

Proposals for the formation of levers of legal regulation of the metaverse and virtual legal relations are not uncommon (Aynur Aydın, 2023; Beliakov, 2016; Jinhee Kim, Arnaldo R. Ramos, Michael Kramer, Ray Gigliotti, 2021; Junhyoung Lee, Heungki Min, 2022), but more pragmatic is the vision of creating an electronic jurisdiction and the Model Metaverse Criminal Code as its main element. Modern legal practice shows that laws developed for material property and pre-digital "offline" or analog social relations with the use of technology cannot regulate dematerialised digitalisation in the metaverse. The dematerialisation and anarchy of the virtual electronic environment generates many processes, both positive and destructive, that negatively affect humanity. The opposite movement is quite relevant and natural in a human-centred society: dematerialisation, i.e., the introduction of law, including criminal law, and power in the metaverse and other virtual environments (Aristova, Baranov, Dz'oban, Beliakov, 2019; Guido Noto La Diega, 2021).

The formation of law enforcement practice, including judicial practice, in relation to these social relations has already begun in various jurisdictions around the world. In addition, the following non-governmental organisations are working on technical regulation and the creation of Metaverse standards: The Metaverse Standards Forum, XRSI Child Safety Initiative, W3C, Virtual World Society, Computer Technology Association, Institute of Electrical and Electronics Engineers, International Organization for Standardization, International Telecommunication Union, The Open Geospatial Consortium, Association "Metaverse-UA", World Economic Forum and others.

Today, scientists from different countries are considering several possible areas for legal regulation of the metaverse.

The first direction is based on the method of "symbiosis" of analogue legislation and legal norms to be applied in virtual environments, based on the similarity with the relevant analogue norms. This approach excludes the possibility of granting metaverse objects and subjects an independent or special legal status. Instead, it is proposed to give them the status of "services" and to base their legal regulation on the same principles and foundations used to regulate social relations in analogous legislation (Donets, 2022; Li Yingchun; Lessig, 1999).

The second area is based on the theory and model of the metaverse electronic jurisdiction and the Metaverse Codes (Kostenko, Furashev, Zhuravlov, Dniprov, 2022; Kostenko, 2022). According to the proposed theory, the legal regulation of social relations in the Metaverse requires the development of a comprehensive electronic jurisdiction based on the latest basic legislation, which should include the following key parts: the Metaverse Constitution (the Magna Carta); the general rules, the composition of the laws of the Magna Carta; the Metaverse Common Law; the Metaverse Judicial System; the Code of the Metaverse Grand Electronic Court of Justice; the Act on the Metaverse Electronic Chancery; the regime of cross-border interaction between different metaverses and the analogue world; the Metaverse Code of Fundamental Technical Regulations; the Metaverse Identity Data Management and Security Act; the Code of Non-Proprietary Electronic Assets and Intellectual Property; the Metaverse Electronic Criminal Code; the Metaverse Code of Cyber Defence Regulations; the Metaverse Military Regulations, etc. (Barlow, 1996; Lessig, 1998).

The third direction is based on the corporate metaverse, and the determination of the jurisdiction whose law will apply to relations in the metaverse will depend on the place of incorporation of the service provider company and the location of the users accessing the metaverse (Zlatin, 2023).

In accordance with the principle of nationality, all legal actions taken in the metaverse by citizens of a particular state, even if they are not physically located in that state, are governed by the laws of the territory of the state where the key nodes of the system are located, or where they are registered as a legal entity or business.

The next direction is limited legal interventionism and consists of combining various industrial policies (standards) (The Metaverse Standards Forum, 2023) and specific (departmental, corporate) legislation

to regulate the metaverse. However, the cycle of standards development from technical concept to commercial application is unpredictable, and legislation does not have time to respond to the challenges of the metaverse, and drafting laws "in advance" may become too active an interference in industry technology and business development (Zhao Jingwu, 2022; Chongqing, 2022).

Another direction of metaverse legal regulation is its decentralisation, but not simple, "brutal" decentralisation, but multi-vector decentralisation. In this version, decentralisation and centralisation are not binary concepts and are often interchangeable. It is proposed to apply to the structure of the metaverse the practice of building multi-ranking networks, according to which vertical centralisation leads to the levelling of the network structure and its horizontal decentralisation. Such an algorithm will facilitate the creation of new independent vertically and horizontally integrated networks and nodes of different ranks. However, such multi-vector decentralisation is difficult to implement (Ding Xiaodong).

The metaverse, as a futuristic electronic society, does not yet have clear legal boundaries, and the task of legal scholars is to predict and outline with sufficient certainty the future contours of legal authority for virtual environments. The following issues are the subject of extensive academic debate: what law should be applied in the metaverse and how conflicting legal conflicts should be resolved; whether governmental regulators in the analogue world are capable of regulating the metaverse by applying existing rules; whether offences in virtual environments should be dealt with within the current framework of tort or criminal law, or whether a separate cross-border electronic jurisdiction should be created.

3. Legal Issues of Using Blockchain and Cryptocurrencies in the Metaverse

Blockchain technology is an emerging field that is still in the process of being regulated in the US, EU and other countries. Researchers (Tapscott, 2017) point to five basic principles of blockchain: computational logic, peer-to-peer transfer, irreversibility of records, distributed database, transparency of pseudonyms (account owners) (Victor Chang, Patricia Baudier, Hui Zhang, Qianwen Xu, Jingqi Zhang, Mitra Arami, 2021). The basic standards for blockchain technology are approved by ISO/TC307.

The legal landscape surrounding blockchain technology (Kostenko, Radutnyi, 2022) is complex and varies significantly across jurisdictions in the US (Primavera De Filippi, Morshed Mannan, Wessel Reijers, 2023), the EU (Shaping Europe's digital future, 2021; Blockchain Strategy, 2021), China (Blockchain in China, 2022; China will soon start regulating blockchain companies, 2019; Opinions of the Supreme People's Court, 2022) and the UK (United Kingdom: Blockchain, 2021; Victor Chang, Patricia Baudier, Hui Zhang, Qianwen Xu, Jingqi Zhang, Mitra Arami, 2020). Some countries have established technical standards for blockchain technology to ensure compliance with laws and regulations, while others have banned all blockchain-related applications of cryptocurrencies (ICOs). However, there is still no adopted blockchain platform on which industry hubs and their application layer podcasts should be based, and the distributed nature of blockchain technology poses a challenge to the application of laws across jurisdictions. Most countries are still in a "legal fog", as their regulators do not have " Blockchain White Papers", "Blockchain Development Strategies" or "Concepts for the Implementation of Blockchain in Electronic Public Services" (Zhao Lei, Shi Jia, 2020).

Jurisdiction is important in the resolution of blockchain disputes, especially when regulating cross-border transactions. The principles of personal and territorial jurisdiction can be extended to apply to blockchain disputes over the location of real nodes and virtual blockchain property (Zhihu, 2021), but only from a corporate perspective or within a totalitarian state (Tang Jing, 2019).

In the United States, the use of cryptocurrencies is attracting significant attention from local and federal governments (Kara A. Kuchar, Steven T., 2022). There are two approaches to regulation: some states promote the technology by introducing favourable rules for the use of cryptocurrencies, while others prohibit it. For example, the state of Wyoming has passed legislation (Joseph A. Castelluccio, Matthew Bisanz, Andrew Olmem, 2023) to create a new type of bank to store digital assets and facilitate the creation of DAOs (Stable Token Act) (Special Purpose Depository Institutions Act, 2021; Gray Derrick and J. Scott Searl, Baird Holm, 2022). The Virginia legislature passed a bill (HB 263) that allows local banks to provide virtual currency storage services as long as the bank has appropriate protocols in place for effective risk management and legal compliance (Troutman Pepper, 2022). Nebraska passed the Nebraska Financial Innovation Act, which regulates the creation of digital asset depository institutions and allows them to obtain a state bank charter (Casey W. Kidwell, 2022; Anthonia Isichei, 2021). Arizona State Senator Wendy Rogers introduced a bill (SB 1235) (Joshua Ramos, 2023) to make bitcoin legal tender in the state (Alys Key).

At the federal level, the focus is on the administrative and agency levels, including the SEC, CFTC, FTC and the Treasury Department through the IRS, OCC and FinCEN. At the same time,

despite the significant activity of these agencies in the cryptocurrency space, no real legal regime in the form of regulations has yet emerged. The US Congress has introduced several federal bills to bring more clarity to the cryptocurrency sector. For example, the Responsible Financial Innovation Act (RFIA), which aims to provide regulatory clarity for agencies overseeing digital asset markets. Another bill, known as the Patrick Toomey Stablecoin Bill, would allow three options for issuing payment stablecoins. Another interesting bill is the Virtual Currency Tax Fairness Act, which would simplify the use of digital assets for everyday small purchases.

The lack of a unified view of blockchain regulation creates a situation where assets created on the basis of blockchain and outside the corporate metaverse are assessed as "investments", which are already regulated and may be subject to traditional financial regulatory regimes such as securities, banking, money transmission, etc. In the United States, the FARA Division has issued an opinion that a US online platform must register under FARA in order to "create a virtual entity presence" for a foreign government agency and "reflect that presence" on the company's platform (Robert Kelner, Brian D. Smith, Alex Langton).

The European Union is developing legislation to require cryptocurrency service providers to detect their illegal use. This is particularly relevant to the fight against terrorist financing and other crimes. The draft laws have not yet been adopted, but are already being discussed at various levels of EU government, such as the "Proposal for the Regulation of Cryptocurrencies" (EUR-Lex; Omri; Hadar Y. Jabotinsky). Recently, the EU Parliament and Council approved the Markets in Crypto Assets (MiCA) law, which lays the foundation for a single legal framework for crypto asset markets in the EU, covering a wide range of digital assets, including utility tokens and stablecoins, and their licensing in any EU country. For the first time in the world, the EU will have a single framework for the regulation of digital assets, which will significantly enhance Europe's ability to compete in innovation. The rules for stablecoins will enter into force in mid-2024, while more comprehensive rules for cryptocurrency service providers will enter into force in January 2025.

The People's Bank of China and seven ministries and commissions issued the "Announcement on Preventing Financial Risks of Token Issuance" (Announcement by seven departments, including the People's Bank of China), and the National Development and Reform Commission and other departments specifically issued the "Notice on Correcting Virtual Currency "Mining" Activities" (Notice of Correction of Virtual Currency Mining Activities, 2021) and the "Notice on Further Preventing and Combating the Risks of Rush in Virtual Currency Transactions" (Notice on Further Prevention and Combating the Risks of Rush in Virtual Currency Transactions, 2021). The People's Bank of China's 2021 Notice states that commercial activities related to cryptocurrencies are illegal financial activities (David 2023; U.S. 2015), and foreign cryptocurrency exchanges that provide services to Chinese citizens are also engaged in illegal financial activities (Xiao Naying, Feith, Yu Leimin, Wang Yufeng, 2023).

One of the main problems associated with the use of cryptocurrencies in the metaverse is the complexity of their decentralisation and regulation, which makes it difficult to trace ownership (Tarakçıoğlu, 2021; Tom Sadon 5 Kinds of Crypto Crimes and How to Investigate Them, 2021) and thus encourages criminals to use them for illegal financial transactions and other crimes (Arianna Trozze, Josh Kamps, etc., 2022; Delton Rhodes, 2018).

4. Legal Issues of Using Smart Contracts and NFTs in the Metaverse

Smart contracts are autonomous contracts in which the terms of the agreement between the parties are written directly in code (Sinclair, 2023). In the metaverse, smart contracts can be used for various purposes in online services, such as trading, finance, real estate, healthcare, elections, virtual assets, intellectual property for virtual assets and objects, etc. However, the legal status of smart contracts in the metaverse is still unclear. In some countries, smart contracts are considered legally binding, while in others they have not yet achieved the status of legal contracts. As the use of smart contracts in the metaverse continues to grow, there is a need to develop a clearer legal framework to regulate their use, as case law shows that the scale of crimes involving their use is increasing (Smart contracts: peculiarities of legal support. Hillmont Partners, 2021; SEC Emergency Action Halts ICO Scam). NFTs (non-fungible tokens) are technical elements (code, electronic key) that record a specific state of the blockchain under the control of a specific smart contract (Rakesh Sharma, 2023). The transfer of ownership of an NFT means the transfer of private keys to access and control the NFT smart contract, or a conditional guarantee that the ownership of an NFT is the ownership of an item associated with the NFT (Michael D. Murray, 2022). An NFT is a digital asset that indicates ownership of a unique object or content (a brand), such as a work of art or virtual property. The legal status of NFTs in the metaverse is still uncertain. In some countries, NFTs are considered property, while in others they are not yet recognised as legal assets. NFTs related to

expressive content may infringe or weaken an existing trademark through minor changes (variations), leading to legal disputes over the legality of the trademark (Michael D. Trademarks, 2022).

5. Legal Issues of AI Application in Metaverse

It should be noted that the need for legal application of AI in the metaverse has not yet been raised. At the same time, the issues of technical and legal regulation of AI have been on the public agenda for a long time and are reflected in numerous national strategies for the development of AI (Kostenko, 2022). The key vector of the vast majority of these strategies is the development of scientific potential and the use of AI as a tool for the development of ecology, medicine and education. Of greater concern, however, is the uncontrolled proliferation and use of AI in both civilian (Clark J., 2023) and military (Kostenko, 2022) spheres.

Currently, there is no single national or international legislative act that provides a model (typical) definition of AI and regulates all issues related to its use (Kostenko, 2022). At the same time, the EU is developing a set of general documents aimed at starting to regulate the scope of AI applications and introducing ethical and legal restrictions (Regulation (EU) 2022/2065; Proposal for a Directive of the european parliament; Document 32022D2481).

However, in 2023, after the introduction of ChatGPT (an extended set of machine learning algorithms called Generative Pre-trained Transformer), the most pressing issues of legal and technical regulation of AI technologies, especially in the area of artificial intelligence-generated content (AIGC), became more relevant. For example, with regard to the regulation of AIGC, the People's Republic of China has introduced mandatory labelling, and violation of this requirement is criminalised as the production and distribution of counterfeit banknotes (Rita Liao). Legislators should pay particular attention to the need to immediately establish legal, technical, physical and other restrictions and controls on military autonomous artificial intelligence systems (AAIS), as well as advanced artificial intelligence systems (AGI) and super intelligence systems (ASI), which may be delegated the rights of a military commander to identify and independently destroy targets, including non-military ones (Kostenko, Jaynes, Zhuravlov, Dniprov, Usenko, 2022).

A separate global issue is the legal regulation of the development and application of certain AI elements, namely neural networks such as convolutional networks (CNN) (TechUkraine), recurrent networks (RNN) (Belsky, 2020) and deep belief networks (DBN) (Deep belief network, 2023), as their algorithms are no longer subject to the "countdown".

The problem of legal regulation of AI is extremely relevant today, as it has gone beyond the application sphere and is beginning to have a profound impact on all spheres of society. Of particular concern is the lack of control over the loading of "poisonous input data" or the input of "poisonous data" into deep AI algorithms, both at the stage of algorithm development, at the stage of data processing, and in the mode of generating an output forecast/answer (now commonly referred to as "decision making"), which can lead to a destructive scenario.

6. Legal Problems of Using Virtual Objects in Metaverse

The metaverse is constantly evolving and forms many virtual objects in relation to which legally significant actions are performed: creation, purchase, sale, exchange, lease, gift, bequest, destruction, change of form and appearance, advertising, pledging for loans, sale or licensing of intellectual property rights and related trademarks, copyrights or patents (Safari Kasiyanto, Mustafa R. Kilinc, 2022).

In general, virtual property in the metaverse faces two main problems: a) what legal instrument to apply to determine whether a virtual object belongs to virtual property and to determine the right of ownership in the metaverse; b) what legal instrument to apply to regulate the relationship of ownership and possession of virtual objects (Buletsa, 2022). There is a scientific position on the expediency of applying the numerus clausus principle in property law with regard to virtual objects (Maidanik, 2019; Nekit, 2019; Joseph Raczynski, 2021). It should be noted that virtual objects can be original and unique products, or they can be reliable electronic copies of real physical objects. Today, this is a promising area of technology and business development, allowing cities to be "cloned", for example, the Chinese company 51World has created digital twins of Shanghai and Singapore. NASA successfully uses electronic twins to test and monitor the performance of its spacecraft. Dassault Systèmes has created a virtual model of the human heart, which is being used to develop new medical devices and analyse drug safety. China's Tencent has created a digital twin of Shanghai's hospital network (Amy Frearson).

An integral part of the general legal issues in the metaverse is the need for clear regulation of intellectual property rights such as patents, copyrights and trademarks for intangible objects (assets) in the metaverse, as well as taxation of virtual assets (Jacob). The problem is that today's traditional analogue ownership of physical objects (assets) is limited in its application to virtual objects, as they are inherently not tangible. However, enforcing intellectual property rights in the virtual environment

can be challenging due to difficulties in establishing ownership and proving unauthorised use. The current legal framework needs to be carefully reviewed and adapted to the legal and regulatory challenges of the metaverse (Kostenko, Golovko, 2023).

It is important to create a clear legal framework that protects the rights of intellectual property owners and the freedom of users to create and interact with virtual objects in the metaverse. These rules should be fundamental and affect the use of virtual objects, clarifying their legal status and ownership, which is necessary to avoid legal problems.

7. Legal Problems of Using Virtual Subjects with Special Status – Avatars, Electronic Personalities or Electronic Humanoids

An electronic avatar is data in electronic form that is sufficient to reproduce a prototype of a person – the owner of an electronic avatar – in the metaverse with maximum accuracy and with rights established by law (Kostenko, Mangora, 2022). Electronic avatars or electronic personalities have become a real object of virtual worlds, which can legitimately claim to be a "subject with a special status" in the near future. Today, the scientific community is considering two hypotheses regarding the status of an avatar: according to the first, avatars can acquire a special status of "electronic legal entity" (Stefania Lucchetti), borrowing concepts from the existing principles of the law of physical companies in general analogue law, and according to the second, a special status of "electronic person/digital humanoid", which will be formed in a common international Metaverse Code. Although both options provide avatars with the property of meta-interoperability and legal subjective unambiguity in the cross-border interaction of analogue and electronic jurisdictions, the authors believe that the special status of an "electronic legal entity" is likely to be applied in the first place, which is still quite logical in accordance with the overall technological and evolutionary development of the metaverce.

Today, there is no general concept for the use of avatars in metaverse and other virtual spaces. Most avatars are animated or stylised using visualisation tools provided by metaverse technology platforms. At the same time, avatars that can reproduce a human prototype already have a narrow application in medical research (Ali Nasrallah, Eric Sulpice, Farah Kobaisi, Xavier Gidrol, Walid Rachidi). At the same time as expanding the range of avatars, Chinese tech giant Tencent announced a programme to generate digital human twins based on the Cloud TI machine learning platform as part of the AI+ Digital Intelligent Human Factory project. The digital twin synthesis process is based on real human video and audio data and takes about 24 hours. Five types of digital avatars are offered: 3D realistic, 3D semi-realistic, 3D cartoon, 2D real person and 2D cartoon (Tencent unveiled a platform for creating digital people, 2023).

The problem of legal compliance of the synthesised avatar of an "electronic humanoid" with a real individual prototype naturally arises. It is especially necessary to regulate the issue of ownership and intellectual property of an avatar of an "electronic humanoid", since the avatar may be the personal or joint property of an individual/legal entity or a corporation that provides resources for the functioning of avatars (Tania Su Li Cheng, 2006).

There is a need for appropriate legal regulation of the reaction of the state, regulatory authority or other authorised body to cases of actions directed against the avatar, but which may affect the subject of legal relations (individual, group of individuals, legal entity or association of them, etc.) that is actually behind the avatar, as well as to regulate actions taken by the avatar that may affect other avatars or other subjects of legal relations. When avatars interact, situations may arise in which the law (of a sovereign state or of the metaverse) is violated, just as it would be between legal entities in the real world. Such incidents may constitute a violation of tort or criminal law (Ben Chester Cheong, 2022). This means that the human prototype of the avatar must agree that his or her avatar has a legal personality that is subject to both the laws of the sovereign state and the laws of the metaverse. It is assumed that the separate legal personality of an avatar will not be taken into account in the case of crimes or torts. Instead, the human owner of the avatar prototype, if he or she is the direct ultimate owner, will be determined to have legal personality after the entire complex of damages has been established, both in the analogue world and in the metaverse.

If an avatar has artificial intelligence capabilities, including the ability to make decisions, enter into contracts and control others in the metaspace, there are grounds for arguing that avatars should be given legal personality in the metaspace (Bettina Chin, 2007).

Avatar technologies allow individuals to create an "electronic humanoid" in a form and with functionalities and features of psycho-emotional development fundamentally different from the prototype, which is impossible to achieve or create in an analogue environment. In other words, a human prototype in the metaverse can have one realistic (official) avatar and many anonymous futuristic avatars at the same time. It is the uncontrolled use of anonymous avatars that can lead to many destructive actions for society (Joanna Bryson, Mihailis E. Diamantis, Thomas D. Grant, 2017).

It is clear that the law will be modernised or created to regulate the use of avatars (Yogesh K. Dwivedi, Nir Kshetri, Laurie Hughes, 2023). The regulation of social relations in the metaverse should solve the main task of clearly defining the status of avatars as electronic subjects, as well as their rights, duties and responsibilities.

8. Legal Issues of Using Identification Data in Metaverse

Access to virtual environments is still a simplified process that does not require the fundamental technical and organisational solutions typical of WEB 2.0 technologies. However, the metaverse is a different structural space in which the source of data are virtual subjects or objects, and the key to the metaverse is their identification data. It is through identification data that the user is given rights, duties and responsibilities in the metaverse.

The essence of identification is that a subject or object possesses or is endowed with a certain identifier (attribute) or identifiers (attributes), which it provides to prove its identity. In other words, identification is the process of collecting, verifying and establishing the validity of the attributes of the identification data of a particular subject or object, which results in the unambiguous identification of the subject or object (Kostenko, 2020).

Identification data management is the processes, functions and procedures for obtaining, verifying, registering, storing, using, protecting and destroying identification data of subjects and objects. The subjects of identification data management are natural persons, legal entities or representatives of a legal entity, and the objects of identification data management are artificial intelligence systems and IoT devices (Kostenko, 2021).

Identifying data directly linked to an individual's bio-data (physiological and biological attributes) are of particular legal and social importance, and these data go beyond the traditional understanding of 'personal data' as defined by the General Data Protection Regulation (GDPR), whose main objective is to give individuals control over their personal data and simplify the regulatory environment for international business by unifying regulation across the EU (EU-2016). Technical progress and modern technologies will soon create technical IoT devices (Kostenko, 2021), which will be able to test physiological and biological characteristics of a person online to create a full electronic copy of a person, on the basis of which avatars or electronic humanoids will function and provide a reliable way of identifying and accessing a person to virtual spaces and virtual property.

Identification data and rights to them are the main, most important and fundamental resources and powers of the metaverse, and the structure of cyberspace allows to separate a person's real identity from his or her virtual one. Therefore, professional and scientific debates are intensifying on how to protect identification data, how to analyse and process them, how to determine the subject of collection, analysis and processing of such data, etc., which will lead to proposals for legal regulation.

9. Problems of Application of Law in the Metaverse

Today, the rules and norms of behaviour in the metaverse are still created based on the projection of the physical world and are corporate in nature. However, there is a tendency for public morality to migrate and legal norms to be translated into the metaverse by simulating cosmopolitan electronic social relations in the absence of clear attributes of the electronic state and the metaverse state structure (Zhihu, 2021).

The key problem of the legal regulation of the Metaverse is the need to create a separate global electronic jurisdiction – a new branch of law acceptable to all users, regardless of actual citizenship and registration in a physical country, which will form a two-stage jurisdiction, where the highest level solves the general legal problem inherent in the social relations of the metaverse, and then at another level the legal regulation is completed in the jurisdiction of a particular state or group of states.

Currently, the legal institutions of national legal doctrines have separate levers to regulate the overall processes of digitalisation of society. Different legal doctrines, different jurisdictions, cultural peculiarities and government priorities lead to significant differences in court decisions on virtual technologies.

The judicial system considers cases of "electronic offences" through the projection of current legislation, thus forming the basis for the future electronic jurisdiction of the metaverse.

The factor of restraining the "unethical" development of artificial technologies is still conditional. However, concerns about the uncontrollability of research in artificial intelligence and neural networks have already moved from discussions to the formation of real levers of restriction.

Today, social relations are developing simultaneously in three conditional dimensions: social relations in the analogue world with the use of virtual technologies, social relations in virtual spaces (metaverse), and social relations formed in the common space of the analogue and virtual worlds, taking into account the expansion of the role

possibilities of individuals through the use of avatars or electronic humanoids.

In light of the above, it is advisable to develop Metaverse Law in the following areas:

1. Regulation of social relations between physical entities created in the modern physical (analogue) world with the use of virtual technologies, within current jurisdictions and in a cross-border mode.
2. Regulation of social relations between physical entities created in the modern physical (analogue) world with the use of virtual technologies, and between virtual entities and objects of the corporate metaverse within current jurisdictions and in a cross-border mode.
3. Regulation of relations between virtual entities and objects of a single metaverse and between metaverse of different formations within the electronic jurisdiction and in a cross-border mode.

As mentioned above, a key element of the metaverse's legal regime is the technologically and legally guaranteed identification of an individual and his or her electronic identity – an avatar or an electronic humanoid. To some extent, this can also be applied to metaverse objects in terms of securing their technological and legal status as virtual non-property objects.

The legal problem will be the formation of metaverse crimes by modelling possible crimes exclusively in virtual space and types of state coercion for their commission, as well as the interpolation of classical types of crimes to crimes committed in virtual reality environments (Pınar Bacaksiz).

In fact, today's legal scholars need to personally immerse themselves in one of the available metaverses and study the processes and relationships in the virtual world from the inside of the object of study. Only in this way can a realistic vision be formed of the whole spectrum of social, technical, technological, legal and ethical issues that need to be rationalised and regulated as soon as possible.

10. Metaverse: Model Criminal Code

The current stage of legal development is characterised by the fact that, in the age of information, criminal law is gradually ceding its role to various specialised laws. Of course, the role of criminal law is not diminished by the delegation of criminal law to other areas of specialised law, but this trend is not entirely optimistic. This was effective in the times of the scientific and technological revolution 4.0 and WEB 2.0. With the development of information and communication technologies and WEB 3.0 technologies, it has become evident that the dispersion of criminal law norms creates a legal dysfunction that does not contribute to the quality legal regulation of modern social relations. The Metaverse Model Criminal Code should concentrate the most necessary legal norms for regulating relations in virtual environments (Won Sang Lee, 2022), and it is not exclusively identified with cybercrime laws and does not duplicate traditional criminal codes. The Model Metaverse Criminal Code should be composite, combining many components with significantly different properties, which, when combined, will lead to the emergence of a new sphere of legal regulation of relations that are impossible in the analogue world. In addition, the Metaverse Model Criminal Code will explore the emergence of new torts in the virtual world and their consequences for the subjects and objects of the virtual world and the legal landscape.

Currently, it is difficult to predict the full range of socially dangerous acts and harms that will be perpetrated in the metaverse, and whether the misdemeanours of a human, human prototype, avatar, electronic personality, electronic subject and object will have the elements of a criminal offence. There is no understanding of what types of punishment or state coercion should be applied to socially dangerous acts of a human, human prototype, avatar, electronic personality, electronic subject and object in the metaverse.

Thus, the Metaverse Model Criminal Code may consist of several basic parts, which in turn will consist of relevant sections and articles (Figure 2):

Part 1 – Glossary or list of technical, technical-legal and legal concepts, rules and terms used in metaverse and related specific areas of law.

Part 2 – The law of the metaverse cross-border regime defines the mechanisms for the establishment of jurisdictions of various types, the interaction between analogue jurisdictions, between analogue and electronic jurisdictions, and between electronic jurisdictions.

Part 3 – The general part of the Metaverse Criminal Code defines the types and stages of crimes in analogue, mixed and virtual worlds, subjects and objects of crimes, guilt and its forms, complicity in crimes, punishment and its types, exemption from criminal liability, sentencing, criminal record, repeated crimes, peculiarities of criminal liability of electronic subjects, avatars, electronic humanoids, etc.

Part 4 – The norms and torts of analogue, mixed and electronic jurisdictions define the types of socially dangerous acts or crimes, as well as the criminal penalties to be applied to persons, entities, avatars, electronic humanoids.

Part 5 – Transitional provisions contain interpretations and procedural algorithms for making additions, amendments, application of archaic, national, cross-border legal norms, etc.

Part 1 is intended to form the conceptual and categorical apparatus used in areas of law related to

the metaverse. It is obvious that the vast majority of terminology is of a technical nature and content that does not correlate with legal norms. It is advisable to form an interdisciplinary conceptual and categorical apparatus that will become a single base of norms and definitions, which will facilitate the development of model legal acts for their simultaneous use in different jurisdictions and will encourage national legislators to revise legislation.

Part 2 aims at formulating the main mechanisms for determining or establishing a regime of cross-border interaction between information and communication systems and virtual spaces of different territories and jurisdictions. First and foremost, such mechanisms or algorithms should ensure simple and reliable identification and classification of events in electronic environments, which will allow them to be categorised by territory, physical and electronic jurisdictions. This approach will not only facilitate the identification of jurisdictions, but will also contribute to the transformation of national legal systems by creating appropriate legal institutions to operate in the metaverse.

Part 3. The general part of the Metaverse Criminal Code should contain provisions establishing the principles and general provisions of criminal law, the validity of criminal law in space and time, the definition of the concept of crime, the stages of intentional crime, the characteristics of the subject of the crime, the content of guilt, the concept of complicity, types of multiple crimes, circumstances excluding the criminality of an act, grounds for exemption from criminal liability and from punishment and its serving, general principles of sentencing, etc.

Part 4 is made up of sections (sections which bring together a certain group of offences contained therein and which are similar in terms of the general object of the offence), each of which is a separate criminal provision containing an independent corpus delicti. The provisions of Part 4 define what socially dangerous acts are criminal offences and what penalties are provided for their commission.

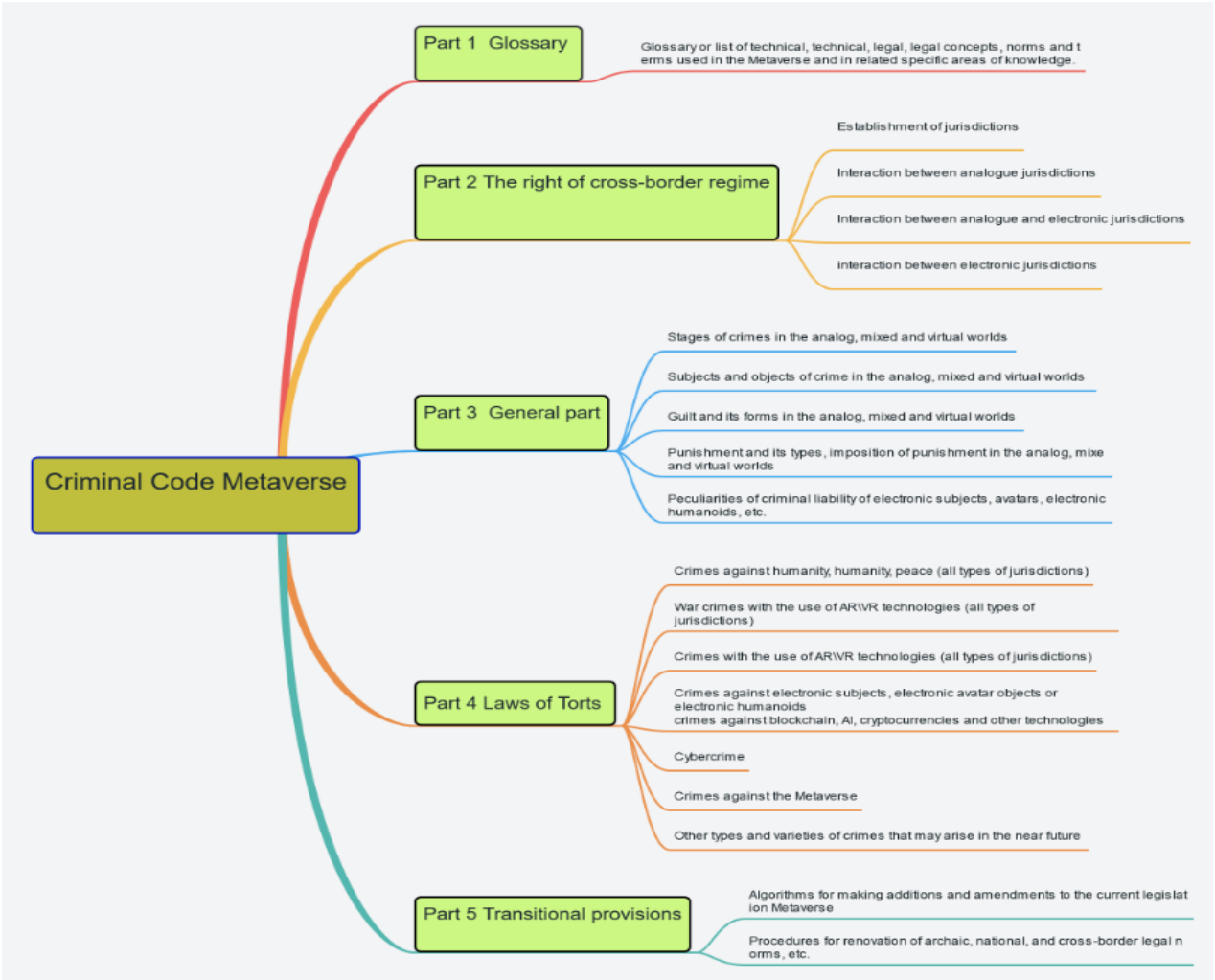

Figure 1. The Metaverse model criminal code

According to the authors, Part 4 should contain the following mandatory sections, the details of which are still subject to legal drafting, namely: crimes with the use of AR/VR technologies (all types of jurisdictions); crimes against people, humanity, peace (all types of jurisdictions); war crimes with the use of AR/VR technologies (all types of jurisdictions); crimes in the field of electronic subjects, electronic objects of avatars or electronic humanoids; crimes in the field of blockchain, AI, cryptocurrencies and other virtual reality technologies; metaverse cybercrime; crimes in the field of identification data; crimes in the field of virtual property, virtual and intellectual property, trademarks, copyrights; crimes against the metaverse; ethical crimes; crimes related to the distribution of drugs, weapons, child pornography, emotional violence; crimes based on racial, national, religious, linguistic and other types of hatred, etc.

The last, 5th Part is intended to formulate instructions, interpretations, algorithms, procedures and other issues of legislation aimed at standardising legislative processes in the field of metaverse electronic jurisdiction, formalising the processes of introducing new regulations, additions, amendments, applying archaic, national, cross-border legal norms etc.

11. Conclusions

The digitalisation of social life and the widespread adoption of metaverse technologies provide users with many opportunities to do electronically what is impossible to do in real life. Among these possibilities are new variations of crimes and offences that cannot be committed in physical reality because of their virtual nature and essence.

The metaverse is no longer just a popular platform for social interaction, commerce and entertainment. Today, the metaverse is beginning to cover more and more areas of human life and influence social relationships. As the metaverse expands and evolves, it creates legal issues that require innovative solutions. It is obvious that social relations in the metaverse are different from the traditional ones inherent in the analogue world. Electronic social relations are in the process of emergence and formation. It is difficult to foresee the full range of legal issues that will need to be addressed by various branches of law, including criminal law. However, with some experience gained in the WEB 1.0-WEB 2.0 era, legal scholars and lawmakers can form a basic vision of the Metaverse Criminal Code model for further development and adaptation in accordance with the formation of virtual spaces.

New torts and their consequences for subjects and objects of the virtual world are emerging. The emergence of new entities such as avatars, electronic humanoids, electronic objects such as crypto-currencies, virtual land, virtual real estate, virtual intellectual property rights, etc. requires new legal approaches and a comprehensive analysis of legal issues in the metaverse and effective proposals for their solution. The development of e-jurisdiction and the Metaverse Model Criminal Code is one such solution that can help create a legal framework for regulating social relations in virtual environments and create a new legal landscape.

This requires legal scholars and scientists from different fields to combine approaches to the legal regulation of different spheres of human life, especially those social relations that are being created today through the use of metaverse technologies.

The Metaverse Criminal Code is a complex and extended legal framework designed to prevent, investigate and prosecute criminal activity that takes place in virtual worlds. As the use of information and communication technologies continues to grow, the need for a comprehensive legal framework to regulate virtual world crime becomes increasingly important to improve understanding of virtual world crime and its impact on society. Legal regulation in the metaverse still requires a great deal of work and research.

References:

Ma Changshan (2018). Legal Reform in the Smart Internet Era, "Legal Research".

Aynur Aydın (2023). Three-dimensional law metaverse law. Available at: https://www.researchgate.net/publication/368469297_THREE-DIMENSIONAL_LAW_METAVERSE_LAW

Beliakov, K. I. (2016). The Conceptual and Methodological Bases o f Regulation the

New Types o f Information Relations: "Virtual Legal Relationships". *Lex Portus*, vol. 2, pp. 47–63. Available at: http://hdl.handle.net/11300/6745

Jinhee Kim, Arnaldo R. Ramos, Michael Kramer, Ray Gigliotti (2021). Let's create Metaverse Law Theories. DOI: https://doi.org/10.13140/RG.2.2.36101.42720/1

Junhyoung Lee, Heungki Min (2022). Review of legal protection measures against security threats related to Metaverse. DOI: https://doi.org/10.21181/KJPC.2022.31.3.321

Aristova, I. B., Baranov, O. A., Dz'oban, O. P., & Beliakov, K. I. (2019). Legal Liability for Offenses in the Information Sphere and the Basics of Information Tort Law: A Monograph, 344 p. ISBN 978-617-697-100-9

Guido Noto La Diega (2021). Internet of Things and the Law Legal Strategies for Consumer-Centric Smart Technologies. P. 390. ISBN 978-042-946-837-7

Donets, A. G. (2022). Doctrinal view on the issues of legal regulation of virtual worlds, "metaverse" private law doctrine: traditions and modernity. Proceedings of the XX Scientific and Practical Conference dedicated to the 100th anniversary of Doctor of Law, Professor, Corresponding Member of the Ukrainian SSR Academy of Sciences, Rector of Kharkiv Law Institute (1962–1987 pp.). P. 3–7.

Li Yingchun. Legal thinking of the metaverse. Available at: https://zhuanlan.zhihu.com/p/436836675

Lessig, L. (1999). Code and other laws of cyberspace. New York: Basic Books.

Kostenko, O., Furashev, V., Zhuravlov, D., & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*, vol. 6(2), pp. 21–36. DOI: https://doi.org/10.46282/blr.2022.6.2.316

Kostenko, O. V. (2022). Electronic jurisdiction, metaverse, artificial intelligence, digital personality, digital avatar, neural networks: theory, practice, perspective. *World Science*, vol. 1 (73), pp. 1–13. DOI: https://doi.org/10.31435/rsglobal_ws/30012022/7751

Barlow, J. P. (1996). Declaration of the Independence of Cyberspace. Available at: https://www.eff.org/cyberspace-independence

Lessig, L. (1998). The Laws of Cyberspace. Taiwan Net '98 Conference. Available at: https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf

Zlatin, V. (2023). Metaverse: problems of legal regulation of processes. Available at: https://juscutum.com/it-i-media-pravo/ua/tpost/x4xvbhgjn1-metavsesvt-problemi-pravovogo-regulyuvan

The Metaverse Standards Forum Where Leading Standards Organizations and Companies Cooperate to Foster Interoperability Standards for an Open Metaverse (2023). Available at: https://metaverse-standards.org/

Zhao Jingwu (2022). The Way of Legal Regulation of Security Risks of the "Metaverse": from Hypothetical Regulation to Prevention of Process Risks. *Journal of Shanghai University*, vol. 5. Available at: https://www.163.com/dy/article/HL0DIH9P0514AGAB.html

Chongqing (2022). Analysis of legal challenges and solutions that may be caused by the "Metaverse". Available at: https://zhuanlan.zhihu.com/p/454673440

Ding Xiaodong. From Arpanet to Blockchain: Legal Regulation of Network Centralization and Decentralization. Available at: https://finance.sina.com.cn/jjxw/2023-05-09/doc-imytcshy1624784.shtml

Tapscott, A., Tapscott, D. (2017). How Blockchain is changing finance. Harvard Business Review, March 1st. Available at: https://hbr.org/2017/03/how-Blockchain-is-changing-finance

Victor Chang, Patricia Baudier, Hui Zhang, Qianwen Xu, Jingqi Zhang, Mitra Arami (2021). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7306205/

Kostenko, O. V., & Radutnyi, O. E. (2022). Blockchain and the Metaverse: Legal Aspects. *Juridical scientific and electronic journal*, vol. 9, pp. 499–506. DOI: https://doi.org/10.32782/2524-0374/2022-9/123

Primavera De Filippi, Morshed Mannan, Wessel Reijers (2023). The alegality of blockchain technology – Oxford Academic. DOI: https://doi.org/10.1093/polsoc/puac006

Shaping Europe's digital future (2021). Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain

Blockchain Strategy (2021). Available at: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy

Blockchain in China (2022). Available at: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_%D0%B2_%D0%9A%D0%B8%D1%82%D0%B0%D0%B5

China will soon begin regulating blockchain companies (2019). Available at: https://cryptonews.net/ru/news/legal/79002/

Opinions of the Supreme People's Court on Strengthening the Judicial Application of Blockchain (2022). Available at: https://www.court.gov.cn/zixun-xiangqing-360271.html

United Kingdom: Blockchain (2021). Available at: https://digital-strategy.ec.europa.eu/en/policies/blockchain-standards

Victor Chang, Patricia Baudier, Hui Zhang, Qianwen Xu, Jingqi Zhang, Mitra Arami (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7306205/

Zhao Lei, Shi Jia (2020). Legal regulation of chain: technical application and legal supervision of blockchain. Available at: http://iolaw.cssn.cn/zxzp/202003/t20200303_5095971.shtml

Zhihu (2021). Building legal norms and systems for blockchain technology. Available at: https://zhuanlan.zhihu.com/p/409245042

Tang Jing (2019). Cina Finance Comprehensive. Legal regulation and blockchain challenges. Available at: https://finance.sina.com.cn/blockchain/roll/2019-01-07/doc-ihqhqcis3747186.shtml

Kara A. Kuchar, Steven T. (2022). CummingsStates Will Continue to Lead in Regulating Digital Assets. Available at: https://www.coindesk.com/layer2/2022/06/08/as-federal-agencies-organize-us-states-continue-to-lead-in-regulating-digital-assets/

Joseph A. Castelluccio, Matthew Bisanz, Andrew Olmem (2023). Wyoming Adopts Stable Token Legislation and Lays the Foundation for a Government-Issued Stablecoin. Available at: https://www.mayerbrown.com/en/perspectives-events/publications/2023/05/wyoming-adopts-stable-token-legislation-and-lays-the-foundation-for-a-government-issued-stablecoin

Special Purpose Depository Institutions Act (2021). Available at: https://wyomingbankingdivision.wyo.gov/banks-and-trust-companies/special-purpose-depository-institutions

Gray Derrick and J. Scott Searl, Baird Holm (2022). Counselor's Corner: What Does the Nebraska Financial Innovation Act Mean for Banks. Available at: https://nebraska-banker.thenewslinkgroup.org/counselors-corner-what-does-the-nebraska-financial-innovation-act-mean-for-banks/

Troutman Pepper (2022). New Virginia Law Permits Banks to Provide Virtual Currency Custody Services. Available at: https://www.troutman.com/insights/new-virginia-law-permits-banks-to-provide-virtual-currency-custody-services.html

Casey W. Kidwell (2022). Becoming a Leader in Cryptocurrency Banking: Nebraska Adopts Financial Innovation Act. Available at: https://www.huschblackwell.com/newsandinsights/becoming-a-leader-in-cryptocurrency-banking-nebraska-adopts-financial-innovation-act

Anthonia Isichei (2021). Nebraska Signs a new Law to Create Crypto Bank Charter. Available at: https://crypto.news/nebraska-new-law-crypto-bank-charter/

Joshua Ramos (2023). Arizona Senator Introduces a Bill to Make Bitcoin Legal Tender in the State. Available at: https://watcher.guru/news/arizona-senator-introduces-a-bill-to-make-bitcoin-legal-tender-in-the-state

Alys Key. Right-Wing Arizona Senator Pushes to Recognize Bitcoin as Legal Tender – Decrypt. Available at: https://decrypt.co/120045/right-wing-arizona-senator-pushes-recognize-bitcoin-legal-tender

Robert Kelner, Brian D. Smith, Alex Langton. DOJ Releases New FARA Advisory Opinions Affecting Digital Media Platforms. Available at: https://www.globalpolicywatch.com/

EUR-Lex. Proposal for a regulation of the european parliament and of the council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

Omri Y. Marian University of Florida Levin College of Law UF Law Scholarship Repository A Conceptual Framework for the Regulation of Cryptocurrencies. Available at: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1703&context=facultypub

Hadar Y. Jabotinsky. The Regulation of Cryptocurrencies: Between a Currency and a Financial Product. *Fordham Intellectual Property, Media and Entertainment Law Journal.* Available at: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1766&context=iplj

Announcement by seven departments, including the People's Bank of China, to prevent tokenization and financing risks (2017). Available at: https://www.gov.cn/xinwen/2017-09/04/content_5222657.htm

Notice of Correction of Virtual Currency Mining Activities (2021). Available at: https://www.gov.cn/zhengce/zhengceku/2021-09/25/content_5639225.htm

Notice on Further Prevention and Combating the Risks of Rush in Virtual Currency Transactions (2021). Available at: https://www.gov.cn/zhengce/zhengceku/2021-10/08/content_5641404.htm

U.S. Attorney's Office. Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts – FBI (2015). Available at: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts

David Z. Morris (2023). The DAO Hack: How a $60M Ethereum Attack Shaped Crypto History. Available at: https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto/

Xiao Naying, Feith, Yu Leimin, Wang Yufeng (2023). Cryptocurrencies recognized as "property" by the courts of Hong Kong SAR and the judicial position of mainland China on this issue. Available at: https://www.kwm.com/cn/zh/insights/latest-thinking/hk-gatecoin-case-and-shanghai-bitcoin-cryptocurrency-recognized-as-property.html

Tarakçıoğlu, Z. E. (2021). Kripto Varliklar ve Ceza Hukuku Sorumluluğu. *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, XI (II), 295–352. DOI: https://doi.org/10.54704/akdhfd.1024708

Tom Sadon 5 Kinds of Crypto Crimes and How to Investigate Them (2021). Available at: https://www.cognyte.com/blog/cryptocurrency-crime/

Arianna Trozze, Josh Kamps, Eray Arda Akartuna, Florian J. Hetzel, Bennett Kleinberg, Toby Davies & Shane D. Johnson (2022). Cryptocurrencies and Future Financial Crime. *Crime Science*, pp. 2–35. DOI: https://doi.org/10.1186/s40163-021-00163-8

Delton Rhodes (2018). Crypto Crimes: ICO Scams, Robbery, and Money Laundering – CoinCentral. Available at: https://coincentral.com/crypto-crimes-ico-scams-robbery-and-money-laundering/

Sinclair, S. (2023). Hong Kong Court Recognizes Crypto as Property. Available at: https://blockworks.co/news/crypto-property-hong-kong#:~:text=While%20Justice%20Linda%20Chan%20determined%20that%20creditors%E2%80%99%20funds,of%20being%20held%20on%20trust%2C%20Hogan%20Lovells%20added

Smart contracts: peculiarities of legal support. Hillmont Partners (2021). Available at: https://hillmont.com/ua/publ/stat/smartkontrakty-osoblyvosti-yurydychnogo-suprovodu

SEC Emergency Action Halts ICO Scam. Litigation Release No. 24079 / March 23, 2018 *Securities and Exchange Commission v. PlexCorps, et al.*, Civil Action No. 17-cv-07007 (2017). Available at: https://www.sec.gov/litigation/litreleases/2018/lr24079.htm

Rakesh Sharma (2023). Non-Fungible Token (NFT): What It Means and How It Works. Available at: https://www.investopedia.com/non-fungible-tokens-nft-5115211

Michael D. Murray (2022). NFT Ownership and Copyrights 14, 15-16. Available at: https://ssrn.com/abstract=4152468

Michael D. Trademarks (2022). NFTs, and the Law of the Metaverse. Available at: https://www.researchgate.net/publication/361938859_Trademarks_NFTs_and_the_Law_of_the_Metaverse

Kostenko, O. V. (2022). Analysis of national strategies for the development of artificial intelligence. *Informatsiia i pravo*, vol. 2(41), pp. 58–69. DOI: https://doi.org/10.37750/2616-6798.2022.2(41).270365

Clark J. (2023). AI Caucus presentation. Available at: https://docs.google.com/presentation/d/1hU9637hH8zWgrBLwhu4AyqM6ic53pDfR-bU7rey8G0w/mobilepresent?fbclid=IwAR0ybonZ3yJrqP3318jZNeOkUh8ydufd5JfKQSXMWHSVHgMDboNm5cvfuyg#slide=id.p

Kostenko, O. V. (2022). The probability of military aggression of autonomous AI: assumptions or imminent reality (analyzing the facts of russian war against Ukraine). *Analytical and Comparative Jurisprudence*, vol. 1, pp. 179–183. DOI: https://doi.org/10.24144/2788-6018.2022.01.33

Kostenko, O. V. (2022). ARTIFICIAL INTELLIGENCE (AI) AND THE METAVERSE: LEGAL ASPECTS. *Juridical scientific and electronic journal*, vol. 8, pp. 301–308. DOI: https://doi.org/10.32782/2524-0374/2022-8/66

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). Available at: https://data.europa.eu/eli/reg/2022/2065/

Proposal for a Directive of the European Parliament and of the council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). Available at: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf

Document 32022D2481. Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance).

Rita Liao. How China is building a parallel generative AI universe. Available at: https://techcrunch.com/2022/12/31/how-china-is-building-a-parallel-generative-ai-universe/?fbclid=IwAR0YN1Qpsd9SLqPEhAjhCUDcgs44BVk59S_HBDJn4VpsW4sBrav6Hblym4k

Oleksii Kostenko, Tyler Jaynes, Dmytro Zhuravlov, Oleksii Dniprov, Yana Usenko (2022). Problems of using autonomous military ai against the background of Russia's military aggression against Ukraine. *Baltic Journal of Legal and Social Sciences*, vol. 4, pp. 131–145. DOI: https://doi.org/10.30525/2592-8813-2022-4-16

TechUkraine. Convolutional neural networks (CNN) (2022). Available at: https://techukraine.net/%d0%b7%d0%b3%d0%be%d1%80%d1%82%d0%ba%d0%be%d0%b2%d1%96-%d0%bd%d0%b5%d0%b9%d1%80%d0%be%d0%bd%d0%bd%d1%96-%d0%bc%d0%b5%d1%80%d0%b5%d0%b6%d1%96-cnn-%d0%b2%d1%81%d1%82%d1%83%d0%bf/

Belsky, O. S. (2020). Recurrent neural networks as a method of predicting physical processes. Available at: https://ela.kpi.ua/handle/123456789/39911

Deep belief network (2023). Available at: https://deepai.org/machine-learning-glossary-and-terms/deep-belief-network

Safari Kasiyanto, Mustafa R. Kilinc (2022). The Legal Conundrums of the Metaverse. *Journal of Central Banking Law and Institutions*, vol. 1, no. 2. DOI: https://doi.org/10.21098/jcli.v1i2.25

Buletsa, S. B. (2022). Virtual property in the metaverse as an object of civil rights. *Scientific Uzhhorod National University Herald. Series: Law*, vol. 1, no. 72, pp. 126–133. DOI: https://doi.org/10.24144/2307-3322.2022.72.21

Maidanik, R. A. (2019). Modernization of real law: basic principle and directions. Real law: priorities and prospects: materials of theses of the Kyiv legal readings. P. 11–19.

Nekit, K. G. (2019). Virtual property: concept and essence. *Law and Society*, no. 2, pp. 37–42.

Joseph Raczynski (2021). The Metaverse is coming: Is the legal market prepared? Thomson Reuters. Available at: https://www.thomsonreuters.com/en-us/posts/legal/legal-metaverse/

Amy Frearson. Digital twins offer "a very powerful way of developing our cities" say experts. Available at: https://www.dezeen.com/2021/07/09/digital-twins-develop-cities-digital-design-architecture/

Jacob W. S. Schneider The Metaverse: Patent Infringement in Virtual Worlds. Available at: https://www.hklaw.com/en/insights/publications/2022/08/metaverse-patent-infringement-in-virtual-worlds

Kostenko, O. V., Golovko, O. M. (2023). Electronic Jurisdiction of the Metaverse: Challenges and Risks of Legal Regulation of Virtual Reality. *Informatsiia i pravo*, vol. 1(44), pp. 105–115. Available at: http://ippi.org.ua/kostenko-ov-golovko-om-elektronna-yurisdiktsiya-metaverse-vikliki-ta-riziki-pravovogo-regulyuvannya

Kostenko, O. V., Mangora, V. V. (2022). Metaverse: legal prospects of regulation application of avatars and artificial intelligence. *Legal Scientific Electronic Journal*, vol. 2, pp. 102–105. DOI: https://doi.org/10.32782/2524-0374/2022-2/23

Stefania Lucchetti. Why Artificial Intelligence Will Need a Legal Personality. Available at: https://lawcrossborder.com/2017/05/22/why-robots-need-a-legal-personality/

Ali Nasrallah, Eric Sulpice, Farah Kobaisi, Xavier Gidrol, Walid Rachidi. CRISPR-Cas9 Technology for the Creation of Biological Avatars Capable of Modeling and Treating Pathologies: From Discovery to the Latest Improvements. Available at: https://pubmed.ncbi.nlm.nih.gov/36429042/

Tencent unveiled a platform for creating digital people (2023). Available at: https://bitexpert.io/news/tencent-predstavila-platformu-dlya-sozdaniya-tsifrovyh-lyudej/

Tania Su Li Cheng (2006). A Brave New World for Intellectual Property Rights. *17 Journal of Law, Information and Science 10*. Available at: http://www5.austlii.edu.au/au/journals/JlLawInfoSci/2006/2.html

Ben Chester Cheong (2022). Avatars in the metaverse: potential legal issues and remedies. Available at: https://link.springer.com/article/10.1365/s43439-022-00056-9

Bettina Chin (2007). Regulating Your Second Life: Defamation in Virtual Worlds. *Brooklyn Law Review*, vol. 72, no. 4, pp. 1303–1349.

Joanna Bryson, Mihailis E. Diamantis, Thomas D. Grant (2017). Of, for, and by the people: the legal lacuna of synthetic persons. *Artificial Intelligence and Law*, vol. 25, pp. 273–291.

Yogesh K. Dwivedi, Nir Kshetri, Laurie Hughes (2023). Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse. Available at: https://pubmed.ncbi.nlm.nih.gov/37361890/

Kostenko, O. V. (2020). Identification data management: legal regulation and classification. *PNAP. Scientific Journal of Polonia University Periodyk Naukowy Akademii Polonijnej,* vol. 43(6), pp. 198–203. DOI: https://doi.org/10.23856/4325

Kostenko, O. (2021). Identification data management (identification): problems of the conceptual and categorical apparatus. Available at: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/102/2590/5544-1

EU-2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Kostenko, O. V. (2021). Paradigms of management of identification data in the light of development of IoT devices and artificial intelligence. *Devices and Artificial Intelligence*, vol. 3, pp. 42–47. DOI: https://doi.org/10.26661/2616-9444-2021-3-06

Zhihu (2021). Legal thinking of the meta-evangelical world. "Legal Practice and Theory". Available at: https://zhuanlan.zhihu.com/p/436836675

Pınar Bacaksiz. Metaverse ve sanal gerçeklik ortamlari karşisinda ceza hukukucriminal law against metaverse and virtual reality environments. DOI: https://doi.org/10.21492/inuhfd.1187521

Won Sang Lee (2022). The Role of Criminal Law in the Metaverse. *Legal Journal*, vol. 42(3), pp. 177–202. DOI: https://doi.org/10.38133/cnulawreview.2022.42.3.177

Received on: 07th of September, 2023
Accepted on: 21th of October, 2023
Published on: 17th of November, 2023