Analysis of Legal Challenges Related to the Prosecution and Punishment of Crimes in the Metaverse

DR Mahmoud Habibitabar[*1],Alireza Hesaie[2], Amir Esmaeili[3]

[1]Department of Law, Saveh Branch, Islamic Azad University, Saveh, Iran
ORCID: 0000-0002-8947-7926
[2] Ph.D. , Department of Law, Faculty of Humanities, Saveh Branch, Islamic Azad University, Saveh, Iran
orcid :0009-0001-6170-7611
[3]Ph.D. , Department of Law, Faculty of Humanities, Saveh Branch, Islamic Azad University, Saveh, Iran

Abstract

With the rapid growth of the metaverse, new opportunities have also given rise to various crimes in this domain. As a result, prosecuting crimes within the metaverse and ensuring punishment transparently—considering users' real identities, data protection, privacy, judicial jurisdiction, and cybercrimes—presents numerous legal challenges. Additionally, determining the legal status of avatars stands as one of the key challenges, suggesting that current laws may be inadequate. This research aims to identify and analyze the legal challenges in the prosecution and punishment of metaverse crimes, to address these issues through a comprehensive and effective approach. The findings indicate that new laws and international cooperation are necessary to tackle these legal challenges. These laws should focus on preventing problems in the metaverse and safeguarding users' rights within this virtual space. Given the decentralized nature of the metaverse, the role of governments in formulating and enforcing these laws is essential. Ultimately, a comprehensive, international approach is required to prevent legal issues and the harm caused by metaverse-related crimes.

Keywords: Metaverse, Digital Fraud, Virtual Identity Theft, Virtual Sexual Assault, Money Laundering.

DOI Number: 10.48047/nq.2025.23.3.NQ25032 **NeuroQuantology 2025; 23(3): 279-288**

Introduction

The three-dimensional virtual world of the metaverse, with its dynamic and unparalleled interactivity, is rapidly becoming an integral part of human digital life. This space has expanded beyond entertainment and social interactions to encompass diverse activities such as e-commerce, education, culture, and even government services. However, alongside these exciting opportunities, the metaverse also presents new legal and social challenges. One of the most pressing challenges is the emergence of complex digital crimes, ranging from various forms of digital fraud to virtual identity theft, creating a host of issues. For example, fraudsters may deceive users by selling fake virtual assets, such as virtual real estate or game items. These fraudulent activities can result in the loss of valuable virtual assets and even users' financial information. Virtual identity theft is another prevalent crime in this space. Individuals using fake avatars or unauthorized access to others' accounts can exploit victims, resulting in both financial losses and damage to their reputation and social relationships. Moreover, crimes like virtual sexual assault and psychological abuse introduce new dimensions of challenges in the metaverse. While these crimes occur in the virtual world, they have significant psychological effects on the victims. Virtual sexual assault may involve inappropriate behavior toward users' avatars, leading to feelings of insecurity and fear. Psychological abuse, such as insults, threats, and hostile behavior, also threatens users' mental well-being. The lack of clear laws to address these crimes makes legal prosecution difficult. However, the legal challenges of the metaverse extend further. Due to its global nature and the presence of users from various countries, determining judicial jurisdiction for handling crimes is complex. The absence of comprehensive international agreements on transnational crimes has left criminals in a state of impunity. Additionally, the protection of personal data and privacy, given the vast amount of information shared in the metaverse, is of critical importance, as misuse of this data could have severe consequences for users. Moreover, data security in this virtual space is at risk due to the lack of precise regulations. As a result, users are vulnerable to potential dangers because current

eISSN 1303-5150

laws cannot address the complexities of cybercrimes. Therefore, extensive legal reforms are necessary to resolve this issue. The development of new regulations that account for the unique characteristics of the virtual world is essential to protect users' rights in this space. These reforms could help create a safer and more reliable environment for all users.

1. Concept, Features, and Philosophy of the Metaverse

The concept of the metaverse was introduced decades ago through a novel, and many studies have since focused on assessing its feasibility and potential. The metaverse is a virtual world that can be accessed through various technologies, offering users numerous capabilities, including interaction with others and participation in activities typically conducted in the real world. At the time of its introduction, the metaverse was considered an unattainable idea because most of the advanced technologies needed for its realization did not yet exist. However, the continuous evolution of technology over the years has made the metaverse possible, allowing stakeholders to better understand its key aspects and potential. Consequently, it is no surprise that the concept has captured the attention of businesses, including multinational corporations. Still, Facebook's rebranding to Meta, signaling its commitment to promoting the metaverse, was a significant milestone. This rebranding has greatly enhanced the metaverse's popularity and continues to be a major topic of global discussion. The successful realization of the metaverse requires the convergence of various advanced technologies, including artificial intelligence, virtual reality, augmented reality, the Internet of Things, cloud computing, and blockchain. Among these, virtual reality is arguably the most crucial, as it powers the metaverse and provides unique features that are highly sought after by users. While other technologies such as artificial intelligence, the Internet of Things, cloud computing, and blockchain are also essential to the metaverse's development, they are primarily concerned with the background infrastructure and may be less visible to consumers. More importantly, these technologies can be used both individually and collectively. Given the separate functionalities each technology offers and the proposed features of the metaverse, it is likely that they will be used together to bring the metaverse to life. Despite the potential these technologies offer, the metaverse is still fundamentally limited by the current state of available technology. Therefore, researchers and developers specializing in the metaverse must continually work on advancing the technologies that will support it. (Mousavi & Abadian Azarkhvarani, 2023: 4)

1.1. Definition and Features of the Metaverse

The metaverse is a collection of multidimensional, simulated, semi-intelligent, connected spaces based on information technology, where social, economic, scientific, and other interactions are conducted in a combined manner through avatars and intelligent humans. All interactions occurring in the physical world are transferable to the metaverse. The presence of intelligent agents, along with high-level graphic and simulation capabilities, adds dynamism and appeal to these spaces. When a real or legal entity enters the metaverse, it essentially creates and develops an enhanced, flexible, and agile representation of its physical existence. The use of electronic tools in the metaverse has eliminated the specific limitations of the physical world and replaced them with dynamic existences and interactions. In the metaverse, individuals can easily communicate with people from different countries, join various communities, follow their interests, and create foundations to attract collaboration in new activities. Entities in the metaverse are categorized into two types: the first category includes hybrid entities that enter the metaverse from the physical space, such as businesses that operate physically in the real world and also establish a presence in the metaverse. These entities typically join the metaverse to expand their activities, market, and manage their electronic and virtual affairs. The second category consists of native metaverse entities that originate purely in the virtual space, such as businesses based on unique tokens or cryptocurrencies, which have no prior existence in the physical world and have emerged in virtual spaces. Over time, the number of native metaverse entities will increase, further fueling the development of differences between the metaverse and the physical space. The connection of humans, the flexibility of spaces, the agility of actions, and other characteristics are considered among the positive features of the metaverse. (Hosseinzadeh, 2023: 10)

1.2. Key Features of the Metaverse

The metaverse is an all-encompassing, immersive

eISSN 1303-5150

virtual space that offers a rich and realistic experience for users. This virtual world transcends the limitations of time and space in the real world, creating a parallel space-time continuum where users can freely travel between different worlds. One of the key features of the metaverse is its sustainability and independence. The platform maintains a self-sustaining, stable economic ecosystem, while also being flexible and open. This delicate balance facilitates growth and development. Additionally, interaction and collaboration in the metaverse allow users to easily move between different worlds and exchange their digital assets effortlessly. This capability ensures a seamless, uninterrupted experience. Given the number of users and the complexity of interactions, the metaverse has high scalability and the ability to expand. The platform can easily adapt to increases in users and avatars without a decline in performance. Diversity and heterogeneity are another feature that distinguishes the metaverse. This space supports a variety of virtual environments, different devices with distinct user interfaces, structured and unstructured data, and multiple communication methods. Furthermore, the metaverse respects the psychological diversity of its users and offers a personalized experience. (Mohammadi Hosseini, 2023: 7)

1.3. Philosophy Behind the Creation of the Metaverse

Humans have always been inclined toward creation and innovation, and this tendency forms the foundation of the concept of the metaverse. It is a visionary idea about how a virtual world can simulate various aspects of our lives and social interactions. The discourse on the metaverse and its global societal impacts, particularly following Mark Zuckerberg's new definition, has been increasing among researchers. Zuckerberg describes the metaverse as an immersive, unified ecosystem in which the boundary between the real and virtual worlds dissolves. Users can share simulated experiences using avatars and holograms, engaging in social and work-related interactions. However, the precise definition of the metaverse is still debated among scholars and has not been fully determined. Some consider it a boundary layer between individuals and reality, where people can experience various activities in a 3D virtual world through augmented and virtual reality. The metaverse is a concept that can have multiple definitions, but currently, it is recognized as a virtual world (or perhaps semi-virtual and semi-real) that functions similarly to the real world. This space provides an environment where users can participate in social activities and interact with one another. (Darabpour, 2023: 69)

2. Crime in the Metaverse

In today's business world, unfortunately, we are witnessing activities that lead to financial violations and fraud. Some companies, with enticing and unrealistic promises, direct people's investments toward fake and illegal projects. One of the most common types of fraud focuses on virtual real estate and advanced technologies. These companies attract investors by promoting projects related to artificial intelligence and virtual reality, drawing them in with promises of high returns. However, in the end, the gathered funds are pocketed and disappear, leaving no trace of the promised projects. Such types of fraud undermine investors' trust and require close supervision and legal action to prevent such violations from recurring.

2.1. Types of Crimes in the Metaverse

Crimes in the virtual world of the metaverse encompass a wide range of illegal activities, which can be classified into three main categories: financial crimes, crimes against individuals, and cybercrimes. Financial crimes include the theft of virtual assets and fraud through digital currencies and virtual assets, directly impacting users' wealth and assets. Cybercrimes represent a significant threat, involving unauthorized access to confidential data and the use of malicious software to infect virtual environments, jeopardizing user security, privacy, and virtual infrastructure. Crimes against individuals include virtual harassment, defamation, and threats, which can have negative psychological and emotional effects on victims. Understanding this broad spectrum of crimes in the metaverse is essential for ensuring security and protecting users in this virtual world.

2-1-1- Financial Crimes

Financial crimes are often defined as crimes against property, involving the illegal transfer of money or other forms of property belonging to someone else. Common financial crimes include fraud, wash trading (a deceptive trading activity where a trader or a group of traders simultaneously buy and sell an asset to create false trading volume and liquidity, which will be explained further below), money laundering, and others. These crimes not only harm investors and users but also pose a specific threat and challenge to the current economic environment.

eISSN 1303-5150

With the recent development of Web3, financial crimes in the metaverse ecosystem have gained a more diverse and complex meaning. Based on the use of blockchain in the metaverse, many criminals have found new opportunities for illegal profits, including money laundering, identity theft, and fraud. The lack of effective regulations on blockchain or Web3 may turn the metaverse into a hub for criminal activities, promoting financial crimes such as fraud, code abuse, wash trading, money laundering, and illegal services and stores. Wash trading is a market manipulation behavior that has emerged in traditional financial scenarios [and is considered a financial crime in most countries]. Generally, it refers to the repeated trading of assets to provide misleading information to the market. Wash trading inevitably leads to increased (fake) trading volume and creates a false sense of prosperity. In the metaverse's economic system, wash trading primarily occurs in native cryptocurrencies, ERC20 token markets, and NFT markets. Many exchanges have been accused of inflating their trading volume through wash trading. In August 2020, Coinbit, South Korea's third-largest cryptocurrency exchange, was accused by the police of faking more than 99% of its trading volume.

In the metaverse NFT market, wash trading is also very common. According to Elliptic (a blockchain data analytics platform), 95% of all activities on the decentralized marketplace Lux Rare NFT (an Ethereum-based non-fungible token marketplace) are related to wash trading. Two main scenarios of NFT wash trading have been observed so far: one is fake trading volume to acquire a new NFT collection, similar to the wash trading of ICO tokens for public offerings.

One of the requirements for validating an NFT collection on the centralized trading platform OpenSea (OpenSea is a decentralized marketplace for buying and selling digital art and NFTs. Since it works with various blockchain networks, it can be connected to multiple cryptocurrency wallets, provided they are compatible with one of the networks supported by OpenSea) is a minimum transaction volume of 100 ETH, which may be difficult for newly launched collections. This requirement seems to encourage fake transactions, where artificial transactions are carried out between several accounts controlled by attackers to artificially increase the transaction volume. Another main scenario of NFT wash trading is obtaining other cryptocurrency rewards through wash trading in NFT transactions. The site Chainalysis reported an explicit dual trade of the same three NFTs between two wallets, amounting to nearly 650,000 ETH in transactions and a transaction fee of 114 million. They reached approximately 185.5 million tokens from the NFT trading platform, which brought in nearly $71 million in profit. Therefore, wash trading traders impact the valuation of metaverse assets and even manipulate the metaverse market. (Jiajing et al, 2023) Identifying and counting wash trading is very challenging. Current main methods of wash trading rely on transaction data. Some works build a transaction network by abstracting the transfer relationships between users and using network topology theory to analyze and identify wash trading activities. For example, Victo and colleagues proposed a wash trading detection method for decentralized exchanges based on identifying loops and cycles in the network. This method found various wash trading structures and volume manipulation in IDEX and EtherDelta with a total value of 159 million dollars. Alternatively, Serniles and colleagues proposed three methods for flagging suspicious NFT wash trading activities, including closed-loop token transactions, closed-loop value transactions, and high trading volume. (Victo, 2021)

2-1-2- Crimes Against Individuals

Crimes against individuals in the metaverse include behaviors that directly negatively impact the mental and physical health of users. Eavesdropping and the interception of invisible avatars is a concern, where future criminals may find ways to make their presence invisible in the metaverse and use this invisibility to spy on important meetings. Another concern in this technology is individuals' identities. When avatars are used for authentication, a person’s identity and personal information may be copied, stolen, deleted, or manipulated. While biometric authentication may offer a solution to these challenges, the potential for other forms of fraud in this space still exists. On the other hand, sexual harassment has become seriously prevalent in the metaverse. Avatars in the metaverse can engage in sexual harassment. These behaviors raise issues regarding their punishment and which regulations and policies should be applied. How does the metaverse regulate the killing of an avatar by another member of the platform? Countries must take action to protect metaverse spaces to safeguard users from sexual harassment. For instance, the Korea Communications Commission

eISSN 1303-5150

has decided to review cases involving individuals under the legal age. A council addressing these concerns will tackle issues related to violence, inclusion, obscenities, sexual misconduct, and crimes. (Bermejo & Hui, 2022)

2-1-3- Cybercrimes in the Metaverse

Addressing cybercrimes in the metaverse between countries can be challenging due to the complex nature of cross-border investigations and the differing laws and regulations in each country. One of the main ways to address cybercrimes between countries is through international cooperation and mutual legal assistance. This involves sharing information, evidence, and data between law enforcement agencies in different countries. (Maloney & Freeman, 2022)

Another method for addressing cybercrimes across countries is through international treaties and agreements, such as the Council of Europe's Cybercrime Convention, which provides a framework for international cooperation in the investigation, prosecution, and extradition of individuals for cybercrimes. Additionally, organizations like Interpol (International Criminal Police Organization) and Europol (European Union Agency for Law Enforcement Cooperation) play a crucial role in coordinating international efforts to combat cybercrimes. (Gauttier et al, 2022)

3- Legal Challenges of Crimes in the Metaverse

The legal challenges of crimes in the metaverse present unique complexities due to the distinctive characteristics of this virtual space. Companies currently managing virtual worlds have established contracts to provide services to their customers, ensuring adherence to these agreements. These contracts typically specify the rules and regulations for using the virtual world, as well as the rights and responsibilities of the company and users. For example, the terms of service for Minecraft prohibit fraud, hacking, sharing personal information, or engaging in hate speech and incitement to hatred. Roblox's terms of service similarly prohibit the sharing of personal information, engaging in hate speech or cyberbullying, or sharing inappropriate content. For World of Warcraft, the terms of service prohibit cheating, hacking, and sharing personal information, and users are also prohibited from engaging in hate speech or harassing other users. In general, these terms and conditions ensure a safe and enjoyable virtual world for all users while protecting the rights of the company and other users. Similarly, Second Life's terms of service prohibit specific behaviors such as harassment, hate speech, and sharing personal information, and outline the rights and responsibilities of users regarding virtual assets within the virtual world. According to these terms and regulations, users retain intellectual property rights for any content they create and upload to the Second Life platform. However, by uploading content to this platform, users grant the company behind Second Life a permanent, global, non-exclusive license to use, distribute, reproduce, modify, adapt, publish, translate, perform, and publicly display the content. Additionally, the terms of service specify that users do not have the right to sell or transfer virtual assets outside the Second Life platform. The company, Linden Lab, which owns and supports Second Life, reserves the right to remove or revoke any virtual asset transferred outside the platform. Users must read and understand the specific terms of service for each platform or virtual world before uploading any content or engaging in or committing to virtual assets. (Lal Alizadeh & Mohammadzadeh, 2023: 202)

3-1- Determining Jurisdiction and Legal Responsibility

Establishing legal frameworks to regulate public relations in the metaverse must address many legal issues related to the differences in the regulations of various jurisdictions. Most legal systems are based on ancient regulations that were developed without considering the potential emergence of social interactions using metaverse technologies. In some cases, these laws may regulate specific issues related to the use of information technology, but their scope is often either limited or vague, creating a situation of legal uncertainty. Modernizing national laws to ensure legal compatibility across multiple jurisdictions is often replaced by temporary laws or regulations. Currently, legal entities still have the leverage to regulate the overall digitalization processes within society, using national legal doctrines. Individual cases of "cybercrimes" are considered by the judicial system through existing laws, thus forming a foundation for future electronic justice in the metaverse. Cultural differences and government priorities lead to significant differences in motivations and judgments, and while modern legislation is progressive, it often lacks complete practical application or turns into declaratory laws.

Regulating public relations in the metaverse requires the development of a comprehensive electronic jurisdiction based on the latest constitutional law— the Grand Metaverse Legal

Charter (GLM). In our view, the GLM should include the following key sections:

- Constitution of the Grand Charter
- Public norms, the composition of the Grand Charter laws
- WM Common Law
- WM Judicial System
- WM Electronic Office Law
- WM Cross-border Interaction Mode
- Basic Technical Regulation Law
- Identity Management Certification
- Non-domestic Electronic Asset Law
- Electronic Criminal Law
- Cyber Defense Law
- Military Regulations
- WM Grand Electronic Judicial Law
- Other regulations

Judicial jurisdiction and justice are key elements in the electronic public relations framework within the metaverse. Initially, justice can be based on traditional "analog" justice systems, which transform in accordance with the development of electronic social relationships in the metaverse. Establishing mechanisms to regulate legal relationships in the metaverse must address several legal issues, including the differences in regulations across various jurisdictions governing the use of information and communication technologies, identification procedures, copyright, ownership of non-financial assets, liability for damages, lists of crimes, and mandatory actions by governments to enforce them (Kostenko et al., 2022).

3-2- Digital Evidence Collection

The first step in collecting evidence is gathering data about the occurrence of a crime in the metaverse, which requires identifying sources that may contain such evidence. These sources could be a physical device, an information system, or a service. The entity involved in collecting the evidence (whether law enforcement or experts in electronic evidence collection) must obtain evidence from reliable sources and ensure that it is in a format that can be easily copied while maintaining the original state as an image and preserving the integrity of the data. Metaverse data may contain evidence of traditional real-world crimes due to the interaction between the metaverse and the physical world. Real-world data can guide the investigation when analyzing a case that occurred in the metaverse. Therefore, researchers may need to analyze all evidence from both worlds in some cases.

On the other hand, digital evidence collection procedures in the metaverse are particularly tied to the unique nature of this world. Since the procedures for collecting digital evidence involve three main sources or domains that constitute the metaverse, these are: the user's devices, the servers of service providers, and the metaverse platform itself (El-Kady, 2024).

3-3- Increase in cybercrimes due to the lack of strong laws

As the metaverse continues to evolve and become more immersive, it also becomes increasingly vulnerable to cybercrimes. In this section, we will examine various types of cybercrimes that may occur within the metaverse. These crimes include: 1) Virtual property theft, 2) Identity theft, 3) Cyberbullying, and 4) Phishing.

3.3.1 Virtual Property Theft

Virtual property theft is one of the most common types of cybercrimes in the metaverse. In the virtual world, users can acquire and accumulate virtual assets such as virtual currency, real estate, and in-game items. These assets can have real-world value, making them targets for cybercriminals. This phenomenon can occur through various methods, including hacking, phishing, and social engineering. Cybercriminals may steal login credentials to gain access to a user's virtual assets. They may also use phishing tactics to deceive users into relinquishing their virtual assets. Additionally, virtual property theft can occur through social engineering, where a cybercriminal gains the trust of a user and then steals their virtual assets. Other tactics employed by cybercriminals include creating fake applications or websites to trick users. The theft of virtual goods, such as cryptocurrency, NFTs, or other assets, not only leads to financial loss but also erodes users' trust in the companies managing such services.

3.3.2 Identity Theft

Identity theft is another common cybercrime in the metaverse. In the virtual world, users can create and customize their avatars to represent themselves. These avatars can be highly personalized and may even feature real-world characteristics such as the user's name or likeness. As a result, they can be targeted by cybercriminals looking to steal a user's identity. Even virtual

eISSN 1303-5150

property theft can lead to the loss of real-value assets, such as virtual currency or real estate. (Valentin, 2023)

3.3.3 Cyberbullying

Cyberbullying is another growing concern in the metaverse. In the virtual world, users can interact with one another in various ways, including text chat, voice chat, and even physical interaction between avatars. However, these interactions can also be used for harassment and bullying other users.

3.3.4 Phishing

Phishing is a common cybercrime in the metaverse that involves using deceptive tactics to trick users into disclosing their login credentials or other sensitive information. Phishing attacks can occur through various methods, including email, instant messaging, and social media.

3.4 Data Protection and User Privacy

Digital marketplaces, such as the metaverse, are often data-driven, and in many cases, data becomes a key factor in enhancing market power. Successful companies in data-driven digital markets benefit from a significant advantage derived specifically from the speed, variety, and volume of big data.

From a theoretical perspective, platforms can identify each user's willingness to pay for a particular product or service through extensive and complex data collection, enabling them to implement price discrimination against customers. Digital platforms extract private data and offer different suggestions to each user based on the calculations of the platform's algorithms. Moreover, data and algorithms enable platforms to potentially improve production efficiency by minimizing transaction costs and user searches. Data and algorithms also enhance the quality of services and products offered, which are designed and personalized based on consumer preferences. (Bakhtiyarvand & Ghoboli Derafshan, 2024: 133)

3.5 Complexity of Digital Interactions and the Spiritual Element of Crimes

Due to the emerging nature of metaverse technology, not all legal aspects related to it have been clarified, and the current understanding of its legal challenges is based on assumptions. Until this technology is widely used, it will be impossible to identify all its legal aspects accurately; however, studying and analyzing current challenges can pave the way for further expansion and development of the metaverse. (Abdusatarov, 2023)

Multiple crimes can occur in the metaverse. According to the latest expert findings, all crimes against physical integrity in the metaverse affect the eyes, ears, and nervous system. These actions can be intentional and carried out through the design of malware, or they can be unintentional and occur during activities. Physical harm to users is not always possible through malware design; it can also result from repetitive ordinary actions that affect the users' bodies. (Sümeyr, 2023)

All Islamic sects agree that awareness of the possibility of a crime creates responsibility for the perpetrator. Therefore, ignorance of the criminal outcome, except in specific cases, cannot prevent criminal liability. In this context, if a user intentionally causes harm to another in the metaverse, the responsibility of the perpetrator (the user) is clear. However, if this action is unintentional but there is awareness of the specific probability of its occurrence, the perpetrator can be punished. According to the definition of crime in Article 2 of the Islamic Penal Code, if the acts are deemed criminal based on a specific probability, they cannot be considered unintentional, and due to the existence of a legal element, punishment can be applied to the criminal, even in the absence of intent. (Mohammadi et al., 2024: 11)

3.6 Determining Criminal Liability and Punishment for Metaverse Crimes

Determining criminal liability and punishment for metaverse crimes is another significant legal challenge. Any intentional action in the metaverse that causes harm to users' lives is subject to criminal prosecution. These crimes may involve the punishment of bodily harm, disciplinary action, and blood money.

If periodic mental disturbances occur, and the person enters the metaverse with full consent and later loses their sanity, resulting in harm to other users, this action is also considered an intentional crime. Regarding unintentional crimes, the likelihood of the crime must be taken into account. This criterion should be determined in future legal sources. Therefore, based on the knowledge of the likelihood of a crime, the actions of the person entering the metaverse can be considered either intentional or purely accidental. (Mohammadi et al., 2024: 12)

In general, harm is a violation of an individual's rights. Not all harm has sufficient grounds for criminalization, but serious harm that significantly damages an individual's benefit becomes a criminal offense, justifying the criminalization of

eISSN 1303-5150

harmful actions. Unfortunately, the law often treats emotional harm differently from physical harm. However, the argument that the adverse impact of virtual behavior on victims is insufficient to justify criminalization, considering the real experience and trauma, is valid. The harm caused by virtual sexual assault should undoubtedly be assessed as criminal harm due to the psychological effects it may have. When a person is sexually assaulted in the metaverse, the boundary between offline and online worlds is blurred, and the effects of sexual assault occurring in the metaverse can extend into the real world. Criminalizing based on emotional harm serves to correct the moral imbalance caused by perpetrators. Three main theories of punishment justify the criminalization of virtual sexual assault based on emotional harm: utilitarian, retributive, and expressive theories. The expressive theory of punishment is centered on compensating victims and "correcting [the moral] imbalance" through punishment. (Bellini, 2024)

4. Commercial Laws in the Metaverse

Commercial laws in the metaverse encompass the buying and selling of virtual goods, the establishment of virtual businesses, and brokerage. The implications of the digital world and the metaverse can be profound for business. Companies can use the metaverse for the following purposes:

- Enhancing consumer experiences
- Introducing virtual products that are only available in the metaverse
- Collecting data about new customers
- Marketing physical and digital products and services
- Supporting payments
- Providing hardware and applications that support specific metaverse functions

In the metaverse, it is possible to gain experience and enhance it through buying and selling items. Additionally, personal digital currencies can be created. Regulations can be established for taxation and legal compliance during buying and selling. In this virtual space, criminals may use cryptocurrencies for money laundering. Internet and computer fraud, including scamming, phishing, fraud, and literary theft, as well as inappropriate behaviors such as racism, discrimination, bullying, and indecency, are common in online virtual worlds.

Monetization in the metaverse occurs through buying and selling, as well as making payments with cryptocurrencies and digital tokens. Some specific and unique products in this space are tokenized and priced in the thousands or even millions of dollars, such as purchasing yachts and land in the metaverse. Users can earn income by selling land, playing games, or creating different outfits. The metaverse is building a growing virtual economy that brings together the real-world economy with opportunities created by virtual infrastructure. The economic opportunities in this space are vast and largely unknown.

The metaverse has created a space for digital property, leading to the creation of a new market for creativity, monetization, and jobs. Tangible tokens, using blockchain technology, such as digital artwork and collectibles, represent ownership of specific assets. (Sharma, Zhou, Huang, and Wang, 2022: 23)

Certainly, the metaverse will extend beyond national borders, requiring multiple regulations. Moreover, while the laws governing the real and virtual worlds are distinct, they are intertwined and may conflict with each other. Legal concepts such as territorial jurisdiction in the real world may face serious challenges. Questions such as, "Which country's governance should apply to an avatar's actions?" and many others will soon become serious challenges, necessitating international policymaking by governments and metaverse regulators.

The metaverse allows businesses to reach customers in a new medium, offering an additional platform for selling products and services. Increased focus on user interactions in the metaverse will compel businesses to enhance their virtual presence through unique experiences, stores, and events. Meanwhile, cryptocurrency-based transactions ensure that purchases in the metaverse are secure and quick, and translate into real-world ownership of products. This provides businesses with a more significant online presence and offers more ways for consumers to engage with their favorite brands.

The metaverse offers new revenue models for existing businesses as companies are no longer limited to the physical world. Businesses can now sell various items and experiences in the metaverse, such as clothing for user avatars, NFTs, real estate, advertising space, immersive experiences, and educational courses. As the metaverse continues to develop, new revenue models emerge, making it an excellent space for companies seeking growth. (Shah Abadian et al., 2023: 124)

eISSN 1303-5150

Conclusion and Recommendations

Pursuing and punishing crimes in the metaverse faces numerous legal challenges that require a new approach in criminology and law. The lack of transparency regarding users' real identities behind virtual avatars, data protection, and privacy, jurisdictional authority, applicable laws, cybercrimes, and intellectual property violations are among the most significant challenges. Additionally, determining the legal personality of avatars and their responsibility for crimes is another legal challenge in the metaverse. These challenges indicate that existing laws may be insufficient and that new regulations and international cooperation are necessary to criminalize and punish metaverse-related crimes. Given that users are located in different countries, determining which jurisdiction and legal system should apply presents a major challenge for law enforcement. Crimes in the metaverse include hacking, identity theft, financial fraud, and cyberbullying, which occur within this virtual environment. Due to the virtual nature of the metaverse, new laws and regulations are needed to protect users from these threats. Additionally, gathering digital evidence in the metaverse presents new challenges for law enforcement. The metaverse is a space where criminals can easily steal users' digital identities and access their assets. Given the virtual nature of the metaverse, protecting users' data and privacy in this space creates new challenges. One of the most critical challenges is collecting digital evidence, as doing so in a virtual environment is significantly more difficult. Moreover, determining punishments for crimes in the metaverse is highly complex, given the virtual nature of this environment.

Recommendation

To address the legal challenges posed by crimes in the metaverse, several solutions can be implemented. One of the most important solutions is to formulate new laws and regulations that can effectively protect users from potential threats. International cooperation is also crucial in combating crimes in the metaverse, as this space operates globally. Digital evidence collection and determining punishments for crimes in the metaverse are also critical solutions. Protecting users' data and privacy in the metaverse must be prioritized as well. By utilizing advanced technologies such as artificial intelligence and blockchain, users can be better protected from crimes. Finally, educating and raising awareness among users about the dangers of the metaverse and how to protect themselves is one of the most important preventive measures for crime in this space.

References

Farsi Sources

- Bakhtyarvand, Mostafa & Qabouli Deraafshan, Seyed Mohammad Hadi, 1403, "The Impact of Metaverse Features on Antitrust Market Power Analysis," *Encyclopedia of Legal Economics*, Vol. 31, No. 25, p. 133.
- Hassanzadeh, Mohammad, 1401, "Metaverse and the Fate of Information Systems," *Quarterly Journal of Information Management Sciences and Technologies*, Vol. 8, No. 1, p. 10.
- Darabpour, Mohammad Reza, 1402, "Metaverse: What It Is and the Legal Challenges (Management, Individuals, and Property)," *Quarterly Journal of New Technology Law*, Vol. 7, Issue 4, pp. 69-70.
- Shah Abadian, Ahad, Hadadi, Mohammad Hassan, Marzi Elmdaari, Jabraeil, 1402, "Exploring Opportunities in E-commerce," *Scientific Quarterly Journal of Islamic Marketing Research*, Vol. 2, No. 2, p. 124.
- Laleh Alizadeh, Mohsen & Mohammad Zadeh, Zahra, 1402, "Identifying Legal Challenges of Businesses in the Metaverse Using Delphi Method," *Transformation Management Research Journal*, Vol. 15, No. 2.
- Mohammadi, Shabnam, 1402, "Reviewing Architecture, Standards, Benefits, and Challenges in the Metaverse," *International Web Research Conference Proceedings*, Vol. 9, p. 7.
- Mohammadi, Neda & Khordmandi, Saeed & Pour Karami, Javad, 1403, "Criminal Responsibility of Users in the Metaverse for Physical Injuries from the Viewpoint of Islamic Jurisprudence," *Journal of Medical Jurisprudence*, Vol. 16, No. 46.
- Mousavi, Seyed Ramin & Abedian Azar Khavarani, Niloufar, 1402, "The Impact of Artificial Intelligence and Metaverse Innovations on Modern Banking," *Quarterly Journal of New Research Approaches in Management and Accounting*, Vol. 7, No. 90.

English referencesa

- 1.Abdusatarov, Jaloliddin. (**2023**) "Issues

eISSN 1303-5150

That Need to Be Resolved When Developing the Legal Framework Of International Private Law Relations In Metaverse." World Bulletin of Management and Law 21.

- 2.Bellini, Olivia, 2024, Virtual Justice: Criminalizing A tual Justice: Criminalizing Avatar Sexual Assault in Meta atar Sexual Assault in Metaverse Spaces,VOL 50, Isse 1.
- 3.Bermejo Carlos, Hui Pan, 2022, Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse, Hong Kong University of Science and Technology.
- 4.El-Kady Ramy Metwally, 2024, Investigating Forensic Evidence in Metaverse: A Comparative Analytical Study, Police Academy, Egypt, Chapter 12.
- 5.Freeman, G., & Maloney, D. (2021). Body, Avatar, and Me: The presentation and perception of self in social virtual reality, Proceedings of the ACM on Human-Computer Interaction. 4(3).
- 6.F. Victor and A. M. Weintraud, (2021) "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges", *Proc. ACM Web Conf.*.
- 7.Gauttier, S.; Simouri, W., & Milliat, A. (2022). When to enter the metaverse: business leaders offer perspectives. Journal of Business Strategy. ahead-of-print. doi.org/10.1108/JBS-08-2022-0149.
- 8.Haber, Eldar, 2024, The Criminal Metaverse, Indiana Law Journal, Vol 99.
- 9.Jiajing Wu; Kaixin Lin; Dan Lin; Ziye Zheng; Huawei Huang; Zibin Zheng, 2023, Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities, Published in: IEEE Open Journal of the Computer Society (Volume: 4).
- 10.Kostenko, Vladimir Furashev, Dmytro Zhuravlov & Oleksii Dniprov, 2022, GENESIS OF LEGAL REGULATION WEB AND THE MODEL OF THE ELECTRONIC JURISDICTION OF THE METAVERSE, PUBLISHED BY THE FACULTY OF LAW, COMENIUS UNIVERSITY BRATISLAVA, Vol. 6.
- 7.Simone, Federica di, 2023, THE METAVERSE: ISSUES REALTNG TO CRIMINAL LAW, *roceedings of the International Scientific Conference "Social Changes in the Global World"*, *1*(10).
- 8.Sümeyra A, Erkan A, and Kapidere M. "Spor Eğitiminde Metaverse." Egitimde Metaverse: Kuram ve Uygulamalar, 2023.
- 9.T. Sharma, Z. Zhou, Y. Huang, and Y. Wang (2022), “” it’s a blessing and a curse”:Unpacking creators’ practices with non-fungible tokens (nfts) and their communities,” arXiv preprint arXiv: 2201.13233.
- 10.Valentin, Alexandru, 2023, Cybercrimes in the Metaverse: Challenges and Solutions, Faculty of Business Administration, Bucharest University of Economic Studies, Romania, Vol.X.