Research article
UDC 34:004:343.9:004.9
EDN: https://elibrary.ru/ypsxqo
DOI: https://doi.org/10.21202/jdtl.2025.8

Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development

Marina A. Efremova ✉

Lebedev Russian State University of Justice, Moscow, Russia

Evgeniy A. Russkevich

Kutafin Moscow State Law University, Moscow, Russia

Keywords

avatar,
crime,
criminal law,
criminal liability,
criminology,
cybercrime,
digital technologies,
law,
metaverse,
virtuality

Abstract

Objective: to conduct a comprehensive analysis of criminal-legal risks arising in the development of the metaverse as a new digital space of social interaction; to define the concept of the metaverse and assess the possibilities of countering criminal activity in this environment by means of criminal law.

Methods: the research methodology consists of the dialectical method of scientific cognition, analysis, synthesis, and a set of specific legal methods. A systematic approach was applied to study legal phenomena in the digital environment; a comparative legal method was used to analyze foreign experience, and a formal legal method – to interpret regulations and doctrinal provisions.

Results: it has been established that the metaverse attractiveness for various forms of criminal activity is largely due to the user anonymity and the lack of a clear legal regime. The study showed that numerous crimes are already being committed on the metaverse platforms. These include socially dangerous acts related to the dissemination of criminogenic and traumatic information, theft of digital property, criminal money laundering, and attacks against the sexual integrity of a person. The authors identify systemic problems of countering crime in the metaverse, including territorial jurisdiction, user identification, and procedural difficulties of proof.

✉ Corresponding author

Scientific novelty: a comprehensive analysis of the criminal-legal aspects of the metaverse functioning was performed. The article formulated theoretical approaches to the qualification of crimes committed in the virtual space. The work substantiates the need to develop special legal structures for regulating relations in the metaverse. The authors proposed a concept of a multidimensional model of legal protection of relations in the metaverse based on public-private partnership.

Practical significance: the study results can be used in improving criminal legislation in terms of regulating responsibility for crimes committed in the digital space. The work may help to develop the concept of legal regulation of the metaverse and to create mechanisms for public-private partnership in the field of countering cybercrime. The findings are relevant for law enforcement practice in the investigation of crimes committed using virtual reality technologies.

For citation

Efremova, M. A., & Russkevich, E. A. (2025). Criminal-Legal Issues of Countering Crime in the Metaverse: Current State and Prospects of Development. *Journal of Digital Technologies and Law, 3*(2), 187–202. https://doi.org/10.21202/jdtl.2025.8

Contents

Introduction
1. Concept of the metaverse
2. Crime and the metaverse
Conclusions
References

Introduction

With the expansion of Web 3.0, virtual reality began to develop in a new direction. Since 2021, leading IT companies have been developing the metaverse, a new digital space combining physical reality with the augmented reality (AR) and virtual reality (VR) technologies.

It is believed that metaverse technologies can be widely used in such areas as education, culture, trade, etc. (Lewandowsky, 2024). The Singapore government has already announced that most public services will soon be available through virtual representations of relevant structures in the metaverse[1].

In Russia, attention to the metaverse regulation and legal risks was largely due to the speech of the President of the Russian Federation, Vladimir Putin, in which he stated the

[1] Newar, B. (2022, July 29). Marriages and court cases can be held in the Metaverse. Cointelegraph. https://clck.ru/3MGuS6

need to use the opportunities of the metaverse so that people could communicate, work together, study, and implement joint creative and business projects. Also, the head of state noted that this is a real challenge for technology companies, creative industries, as well as for lawyers who are to develop rules for regulating economic and public relations in the fundamentally new world[2].

According to expert estimates, the metaverse market should reach US$74.4 billion in 2025 and 2,633 million users by 2030[3]. Many of the world's leading brands have already established their presence in the metaverse and begun trading and holding virtual presentations, concerts, and exhibitions. For example, in the Decentraland metaverse, Dolce & Gabbana hosted the first Metaverse Fashion Week, featuring a 20-piece collection[4]. Omoda unveiled a new line of vehicles on the metaverse platform. Visitors submitted applications for a test drive of cars, and sales increased after the virtual dealership was opened[5].

We should agree with A.M. Konstantinov that the digital metaverse is currently being formed as an integrated and multilateral public space, some aspects of which are a challenge for many humanities, including legal theory[6].

It is important to realize that the metaverse is not just another multiplayer computer game. The idea of the metaverse is to create a virtual analogue of the real world, although it will not be limited to this, of course (Narasimhan & Kala, 2024). In the criminal law aspect, the metaverse attracts attention as a new space for social interaction, which can (and in fact already does) serve as a space for criminal activity (Saharan et al., 2023). Indeed, for many socially dangerous attacks provided for by criminal law, virtualization makes little difference in achieving the desired result. Moreover, such a virtual world, which does not have a clear law enforcement system, has obvious advantages for intruders (anonymity, wide reach, etc.) (Marshall & Tompsett, 2023).

One could object that the problem of malicious behavior in the metaverse is far-fetched, does not require legal intervention, and should remain completely within the system of relations between a resource owner and a user. We believe that this is a misconception. Such an elimination from public regulation and protection (the "vicious circle" theory) is relatively suitable for computer games, but not for a virtual analogue

2 Minutes of the speeches of participants of Artificial Intelligence Journey 2021. (2021, November 12). https://clck.ru/3MGuU3

3 Metaverse – Worldwide. Statista. https://clck.ru/3MGuW6

4 Metaverse Fashion week. (2022, April 25). NFT Art. https://clck.ru/3MGuYW

5 Is there a demand for events in metaverses in Russia? (2023, July 29). Sostav. https://clck.ru/3MGuau

6 Konstantinov, A. M. (2023). Gaming norms in legal regulation. Cand. Sci. (Law) thesis. Volgograd. P. 145.

of the real world in which government agencies, commercial and non-profit organizations, and real people operate, albeit through their digital counterparts (avatars) (Singh, 2024).

1. Concept of the metaverse

The term "metaverse" is believed to first appear in Neal Stephenson's novel "Snow Crash" in 1992, showing a virtual world as a continuation of people's physical lives, in which they spent most of their time.

The metaverse is a result of convergence of technologies, the blockchain and the Web.3 named as the key ones. Immersion technology is also one of the main components of the metaverse, used to connect users to the virtual world and interact with its objects (Alawadh, 2023). Immersive technologies ensure a realistic representation of virtual content in the metaverse. The Internet of Things (IoT) is necessary to connect the metaverse with the real world. A network is required for communication and data transmission. It allows users around the world to connect to the metaverse (AlMutawa et al., 2024). Cloud and peripheral computing are required for the distributed storage and processing of the vast amount of data generated by the metaverse. It is important to emphasize that the metaverse allows people to interact as if they are not in the virtual, but in the real world.

Although there is no universal definition of the metaverse, in a broad sense it can be defined as a collective virtual space created by a convergence of augmented virtual reality and the physical world.

2. Crime and the metaverse

The metaverse poses the same systemic problem to criminal law as it does to any branch of law (AL-Tkhayneh, 2023). Conventionally, it can be described as follows: if the metaverse is a digital analogue of the physical world where individuals enter into relationships and engage in harmful behavior using their digital images (avatars), is it possible to extend the existing legal frameworks to both these relationships and this harmful behavior?

Modern literature suggests that any crime, including murder, can be committed in the metaverse. This is a bold idea. To agree with it, one must review many fundamental provisions of criminal law, to form completely different understanding of such key categories as victim, life, death, the subject of crime, etc. Is the Russian legal doctrine ready for this? Probably not.

Currently, crimes related to the dissemination of criminogenic and traumatic information are committed on the metaverse platforms (Gómez-Quintero et al, 2023). To a certain extent, this was expected, since digital technologies have always been attractive for criminal activities related to the distribution of prohibited content (Teodorov, 2023).

As for many criminal acts of this group (Articles 110, 110[1], 110[2], 128[1], 137, 205[1], 205[2], 205[3], 242, 242[1], 280, 280[1], 280[3], 280[4], 282 of the Russian Criminal Code), their implementation in the metaverse does not exclude the possibility of bringing a person to criminal responsibility. The metaverse is just one of many digital platforms (messengers, social networks, multi-user virtual games, etc.) used to disseminate prohibited information (Blake, 2023).

Special attention should be paid to the question whether information about a person's activity in the metaverse is a personal secret within the meaning of Art. 137 of the Russian Criminal Code. Today, the virtual world provides a user with almost limitless opportunities for self-identification and self-expression: one can choose an avatar of any gender, determine their race, age and appearance at one's own discretion. The user can enter into a variety of relationships with other avatars and be active in the metaverse, while assessing the information about it as a personal secret. For example, in the metaverse, users can not only be in a relationship (engage in sexual activity without physical contact), but also get married with an NFT certificate, which serves as an alternative to official registration in the real world. We believe that the collection and dissemination of such information about a real person (provided they correspond to the signs of secrecy) fully fall within the Art. 137 of the Russian Criminal Code.

The possibility of bringing a person to criminal liability for violating the right to freedom of conscience and religion committed in the metaverse (Article 148 of the Russian Criminal Code) is debatable. By its nature, this crime can consist both in the public dissemination of certain information offensive to believers and in the commission of specific actions related to interference in worshipping, ritual, etc. In the first case, the application of Art. 148 of the Russian Criminal Code cannot raise objections. However, in case of other actions one has to agree with several assumptions at once, first of all, with the fact that worship or other religious rite can take place in the metaverse. In addition, it should be recognized that the avatar's behavior in the metaverse has signs of interference in the ritual. Indeed, under certain circumstances, a person who is not aware of the intricacies of a particular religious rite can quite conscientiously assess one's actions as permissible and not creating obstacles to its implementation. But, of course, the key issue is recognizing the very possibility of exercising the right to freedom of conscience and religion in the virtual space.

A broadly discussed problem of crime in the metaverse is the possibility of attacks against sexual freedom and sexual integrity of an individual (Wiederhold, 2022). The key point is that it is not the user who is being "sexually abused", but their avatar, of course[7]. Those who had encountered with this phenomenon noted that they had experienced

[7] Smith, I. (2016, October 30). Even in a virtual world, the harsh reality of sexual harassment persists. NPR. https://clck.ru/3MGumo

a strong emotional shock as a result of such actions. A famous example is the case of Nina Jane Patel, whose avatar was sexually assaulted by four male avatars at once on the Horizon Venues platform. According to her, she experienced a psychological shock. It is indeed noted in the literature that, due to immersive technologies, such actions against an avatar can cause emotional experience comparable to the shock of sexual violence in real life (Chawki et al., 2024).

Another example: in the UK, an investigation was initiated into an incident in the metaverse where an avatar (owned by a child) was attacked, involving manipulation similar to sexual violence. This fact caused a mixed reaction from the public. Many criticized, pointing out that law enforcement agencies should be engaged in criminal prosecution of real attacks on sexual freedom[8].

For the same reasons as with murder, the application of criminal law norms on liability for sexual crimes in relation to avatars of the metaverse seems impossible. An avatar is just a digital image of a person in the virtual world and cannot have sexual freedom, as well as sexual inviolability. At least, that is the case at the moment. Of course, one may assume that over time such digital alter-egos will become inseparable from the real person. Then, we will have to review the object of sexual assault and recognize, as part of a person's sexual freedom, also one's right to choose partners and engage in sexual relations, at one's own discretion and without coercion, using one's avatar in the metaverse (Cheong, 2022). However, this is a question of the future and, probably, not the closest future.

It is important to make a reservation that, under the Russian criminal law, it is already possible to initiate criminal proceedings on indecent acts in the metaverse and in some cases on sexual violence against a person under the age of twelve – provided that the perpetrators were aware of the age of the avatar's owner, of course.

The metaverse ecosystem provides opportunities for the acquisition of "digital property", including virtual land plots, buildings and structures. The three most popular platforms include The Sandbox, Decentraland, and SuperWorld. It is known that the cost of land plots can range from hundreds to millions of US dollars. For example, one of the most expensive "digital real estate" transactions was the purchase of 100 private islands on The Sandbox platform for US$4.3 million[9]. The metaverse users place bets on virtual land plots via trading platforms, and purchasing is much like buying real estate in the real

[8] Camber, R. (2024, January 1). British police probe VIRTUAL rape in metaverse: Young girl's digital persona 'is sexually attacked by gang of adult men in immersive video game' - sparking first investigation of its kind and questions about extent current laws apply in online world. Mail Online. https://clck.ru/3MejXs

[9] META MONEY Most expensive metaverse properties – including $4.3m purchase of EMPTY virtual land. (2022, March 28).The Sun. https://clck.ru/3MGuu6

world. As soon as the buyer purchases virtual land, the transaction is recorded in the blockchain, which in a sense serves as an analogue of making an entry in the real estate registry when making transactions in the real world. Since many of these virtual worlds have a limited number of land plots, as the popularity of the platform grows, so does their value. Cases of illegal acquisition of digital property in the metaverse are also known. For example, a malware program was used to "steal" a land plot worth £10,000[10] from one of The Sandbox platform users.

According to Russian criminal law, it is impossible to steal virtual property. We can only talk about illegal access to legally protected computer information for mercenary reasons (Part 2 of Article 272 of the Russian Criminal Code). However, one should admit how far such a qualification is from the content and focus of seizing the victim's digital assets. After all, this is not so much about the software and technical means of information protection, but rather about taking possession of items that are marketable and often of significant value.

The debate on this issue in modern jurisprudence (Lin et al., 2023), as a rule, points out the dependence of criminal law protection on the regulation of the relevant objects' turnover in civil law. However, given the current situation, there are more and more arguments that such a relationship does not constitute an absolute dependence of one on the other (Bhardwaj, 2024). Perhaps, the recognized secondary nature of criminal law protection can be overcome by developing special rules for the qualification of encroachments on "digital property", with them forming the subject of specific crimes against property. Similar approach is known to be implemented in the explanations of the Russian Supreme Court's Plenum about legalization. If transactions with cryptocurrencies and other digital assets are possible per se, including for the purposes of criminal legalization, then there are no serious obstacles to considering them as an object with a specific value at the time of the criminal encroachment.

As was noted above, the internal economy of the metaverse serves as an effective tool for money laundering (Wu et al., 2023). Metaverses allow, just as in the physical world but with lower risks, to create the appearance of "profitable" economic activity (provision of virtual services, trading in virtual assets, etc.). This has already been highlighted in the legal literature (Mooji, 2024). In general, the provisions of the Russian criminal law (Articles 174, 174[1] of the Russian Criminal Code) can be applied here on common grounds.

The existence of own economy within the metaverse (Wasswa, 2023) raises the question of the applicability of the traditional criminal law liability provisions to crimes in the field of business and taxation. Suppose a person organizes a platform-based cryptocurrency exchange point. Clients visit it using avatars and make payments with the

[10] LAND GRAB I bought £10,000 worth of digital land in The Sandbox metaverse game but it was stolen and sold for £23,000. (2022, January 11). The U.S. Sun. https://clck.ru/3MGuvq

organizer in one form or another. Clearly, in real life such activities are grounds for bringing the person to criminal liability for illegal banking (if a large amount of income is proven). As is rightly noted in the literature, actions to cash out funds may constitute a crime under Article 172 of the Russian Criminal Code, if large-scale income is extracted, since cashing operations can be considered cash services for individuals and legal entities (Gribunov et al., 2023). However, banking operations cannot be carried out in the metaverse, at least from a formal viewpoint.

It is equally difficult to qualify the actions of a person who, having the status of an economic entity, carries out activities (consulting services, design, etc.) not only in the physical world, but also in the metaverse, receiving significant income from the latter. I.A.Khavanova rightly summarizes that national regulators and tax authorities are still trying to comprehend the problems that arise in the metaverse, including those related to determining the moment of income, evaluating transactions of exchanging virtual goods for virtual or fiat currencies. At the same time, she is right saying that the technical impossibility of accurately calculating the tax base and determining the source of income in a space whose integral component is anonymity should not serve as a basis for non-taxation (Khavanova, 2024). Consequently, it is impossible even to raise the question of applying the rules on tax crimes if a person misleads the tax authorities about the income received from activities in the metaverse.

The above list of criminal-legal risks in the metaverse is, of course, not exhaustive. For example, one could also consider the urgent problem of committing corruption crimes using digital objects of the metaverse. However, further presentation of specific examples will add little to the overall picture. It is more important to pay attention to a number of systemic problems of crime prevention in the metaverse.

As is known, the metaverse has no geographical boundaries. Experts are actively discussing the problem of establishing so-called “cyber boundaries”, or the limits of the powers of states in virtual interaction and compliance with “cyber sovereignty”. It is expected that special procedures will be developed for the metaverse to hold individuals accountable for offenses and crimes based on the legislation of those countries with which the relevant metaverse platforms are affiliated[11]. So far, these problems are under development, which creates additional prerequisites for various forms of criminal activity.

There is much debate about whether the real identity of a user of the metaverse should be disclosed in case of an illegal act. This, anyway, is related to the question

[11] Abraham, A. (2022, April 4). Law & Order in the Metaverse. Finextra. https://clck.ru/3MGv2L

of whether the user's real identity should be combined with only one avatar. Obviously, if a user can have only one avatar, additional identification information will be required. Since the legal guarantees of the right to privacy vary from country to country, it is necessary to reach a consensus on what information about their identity should the users provide.

Until now, when creating avatars, users may imitate other people: celebrities or their friends, colleagues, as well as deceased persons. Over time, this can lead not only to ethical, but also to legal problems (Begishev et al., 2023). For example, law enforcement practice may face numerous disputes about protection of honor and dignity, business reputation and good name against actions committed in the metaverse using the victim's biometric data (for example, a peeved student using the biometric data of a professor in the metaverse to create an image of a prostitute or a drug dealer). A fundamental solution is possible by introducing a registration mechanism in the public registry of avatars, where each person may register only one avatar in the metaverse under a unique identifier (Qin et al., 2025). At the same time, if we are talking about the metaverse as an alternative social space in a virtual environment, the creation of such a registered avatar, supposedly, should be linked to the user's biometric data (technically it is already possible now). In other words, at a certain stage in the metaverse development, today's complete freedom to choose a digital image will probably have to be abandoned.

Finally, all the above said, related to the (greater or lesser) applicability of the substantive criminal law provisions to the users' actions in the metaverse, is only valid if we agree that there are procedural and criminological tools to prove a criminal case. This has already been noticed in Russian science. For example, O. A. Zaitsev rightly stated that we have to improve access to technological integrated platforms that facilitate obtaining the necessary data in the infrastructure of a single information space, as well as to change the very concepts of the criminal procedure, as it contradicts modern methods of obtaining evidentiary information. He also rightly noted that we urgently need an improved legal regulation of electronic evidence in proving the guilt (innocence) of a person in committing a criminal act, as well as a greater range of investigative actions to more productively obtain evidentiary information in electronic format (Zaitsev, 2024).

Conclusions

The most predictable answer to all the problematic issues of legal regulation and protection of relations in the metaverse would be to state that the digital analogue of human physical space requires a digital analogue of real-world law. This involves either applying the provisions of legislation by analogy (where this is permissible), or expanding the limits of existing legal structures through interpretation, or, if necessary,

constructing special "digital twins" of legal norms designed specifically for these relations.

However, the simplicity of the solution is not a guarantee of its correctness. Not everything in the metaverse should be regulated or protected by means of criminal repression. As in the physical world, there are areas in the metaverse that should remain outside the legal regulation. Perhaps, we may argue that there should be significantly more such spheres in the metaverse than in real life.

However, it is also clear that one cannot remain in the paradigm of the real law non-interference in virtual relationships (Duranske, 2008; Fairfield, 2012). According to A. A. Smirnov, in the longer event horizon, as the ontological status of virtual worlds is established as a new environment for human existence, there will be a need to create a full-fledged system of legal regulation of life in virtual worlds (metaverses). Based on these considerations, he justifies the need to develop and adopt a Federal Law "On virtual and augmented reality systems"[12].

At the same time, T. Ya. Khabrieva quite rightly points out the general ineffectiveness of exclusively legislative regulation of relations in cyberspace, compared to other mechanisms (Khabrieva, 2018). In this regard, the model of regulation and protection of relations in the metaverse seems promising mainly through the development of framework rules of user behavior (the so-called "soft law" system) and the selective regulation of legal norms of those relations that cannot be regulated in any other way (beyond the boundaries of the well-known "vicious circle"). In order to prevent and effectively counteract crimes, states and metaverse platforms' owners have yet to find a balance between anonymity and the protection of confidential user data. The metaverse platforms cannot remain just a virtual field for user interaction; they must be involved in their interaction to ensure a balance of interests. Therefore, the model of protecting relations in the metaverse from the most dangerous attacks should be multidimensional and based on close cooperation between the state, the IT sector, business, and users.

References

Alawadhi, I. M. (2023). F*uture Cybercrimes in the Metaverse* (pp. 24–32). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch002

AlMutawa, A., Ikuesan, R. A., & Said, H. (2024). Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model. *Future Internet*, *16*(12), 437. https://doi.org/10.3390/fi16120437

AL-Tkhayneh, K. M., Olowoselu, A., & Alkrisheh, M. A. (2023). *The Crime in Metaverse (the Future Scenarios for Crime Patterns and the Prospective Legal Challenges)*. 1–6. https://doi.org/10.1109/snams60348.2023.10375402

Begishev, I., Denisovich, V. V., Sabitov, R. A., Pass, A. A., & Skorobogatov, A. (2023). *Criminal-legal significance of metaverses: collisions in law*. https://doi.org/10.47475/2311-696x-2023-39-4-58-62

[12] Smirnov, A. A. (2022). Forming the system of legal provision for information and psychological security in the Russian Federation. Dr. Sci (Law) thesis. Moscow.

Bhardwaj, A. (2024). *Cyber Fraud Use Cases in the Metaverse* (pp. 106–130). BENTHAM SCIENCE PUBLISHERS. https://doi.org/10.2174/9789815238457124010007

Billcliff, T. (2023). *Cybercrimes in the Metaverse: Challenges and Solutions*. https://doi.org/10.19107/cybercon.2023.28

Blake, J. (2023). *Online Crime in the Metaverse* (pp. 66–77). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch004

Chawki M., Basu, S., Choi, K.-S. (2024). Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws*, *13*(3), 33. https://doi.org/10.3390/laws13030033

Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedie. I*nternational Cybersecurity Law Review*, *3*, 467–494. https://doi.org/10.1365/s43439-022-00056-9

Duranske, B. T. (2008). *Virtual Law. Navigating the Legal Landscape of Virtual Worlds*. Chicago, Illinois: ABA Publishing, American Bar Association.

Fairfield J. A. T. (2012). Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life. *Berkeley Technology Law Journal, 27*.

Gómez-Quintero, J, Johnson, Sh. D., Borrion, H., & Lundrigan, S. (2023). *A scoping study of crime facilitated by the metaverse*. https://doi.org/10.31235/osf.io/x9vbn

Gribunov, O. P., Nikonov, P. V., Parkhomenko, S. V., Rogova, E. V., Shikhanov, V. N. (2023). *Digital currency and digital financial rights as an object and means of committing crimes*. Irkutsk: Irkutsk Law Institute (branch) of the University of the Russian Prosecutor's Office.

Khabrieva, T. Ya. (2018). The law facing the challenges of digital reality. *Journal of Russian Law*, *9*(261), 5–16. https://doi.org/10.12737/art_2018_9_1

Khavanova, I. A. (2024). The metaverse: the problem of adapting tax and legal structures. *Journal of Russian Law*, *7*, 78–93. https://doi.org/10.61205/S160565900029634-1

Lewandowsky, P. (2024). Cybercrime in the Meta-Universe. *Journal of Social Science and Humanities*, *6*(8), 5–8. https://doi.org/10.53469/jssh.2024.06(08).02

Lin, K.-X., Wu, J., Lin, D., & Zheng, Z. (2023). A Survey on Metaverse: Applications, Crimes and Governance. In *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan* (pp. 541–549). https://doi.org/10.1109/metacom57706.2023.00097

Marshall, A. M., & Tompsett, B. (2023). The metaverse – Not a new frontier for crime. *WIREs Forensic Science*, *6*(1), e1505. https://doi.org/10.1002/wfs2.1505

Mooij A. (2024). *Regulating the Metaverse Economy*. Springer Briefs in Law. Springer.

Narasimhan, P., & Kala, N. (2024). Securing the Metaverse: AI-Driven Solutions for Cyber Security, Privacy, and User Trust. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(6), 1890–1918. https://doi.org/10.32628/cseit241061238

Qin, H. X., Wang, Y. & Hui, P. (2025). Identity, crimes, and law enforcement in the Metaverse. *Humanit Soc Sci Commun*, *12*, 194. https://doi.org/10.1057/s41599-024-04266-w

Saharan, S., Singh, S., Bhandari, A. K., & Yadav, B. (2023). The Future of Cyber-Crimes and Cyber War in the Metaverse. In H. N. Elshenraki (Ed.), *The Age of the Metaverse* (pp. 126–148). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch007

Singh, P. P. (2024). Cyber Crimes in Metaverse. *International Journal of Science and Research*, *13*(2). https://doi.org/10.21275/mr24130195237

Teodorov, A.-V. (2023). Cybercrimes in the Metaverse: Challenges and Solutions. In *International Conference on Cybersecurity and Cybercrime*, 10 (pp. 209–215). https://doi.org/10.19107/cybercon.2023.28

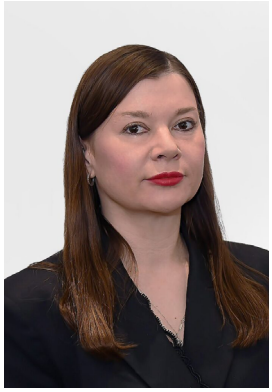
Wasswa, S. (2023). *Predicting Future Cybercrime Trends in the Metaverse Era* (pp. 78–113). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch005

Wiederhold B. K. (2022). Sexual harassment in the metaverse. Cyberpsychology. *Behavior, and Social Networking*, *25*(8), pp. 479–480.

Wu J., Lin K., Lin D., Zheng Z., Huang H .and Zheng Z. (2023). Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. *Open Journal of the Computer Society*, *4*, 37–49.

Zaitsev, O. A. (2024). Features of criminal-procedural evidence in the context of digitalization. J*ournal of Russian Law*, *8*, 93–112. https://doi.org/10.61205/S160565900030639-6

Authors information



Marina A. Efremova – Dr. Sci. (Law), Professor, Head of the Department of Criminal-legal Disciplines, Kazan branch of Lebedev Russian State University of Justice
Address: 7a 2nd Azinskaya Str., 420088 Kazan, Russia
E-mail: crimlaw16@gmail.com
ORCID ID: https://orcid.org/0000-0003-1076-2765
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57189299773
WoS Researcher ID: https://www.webofscience.com/wos/author/rid/E-6250-2016
Google Scholar ID: https://scholar.google.com/citations?user=mLPofnMAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=630526

Evgeniy A. Russkevich – Dr. Sci. (Law), Associate Professor, Professor of the Department of Criminal Law, Kutafin Moscow State Law University
Address: 9 Sadovaya-Kudrinskaya Str., 125993 Moscow, Russia
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
WoS Researcher ID: https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – March 8, 2025
Date of approval – March 26, 2025
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:343.9:004.9
EDN: https://elibrary.ru/ypsxqo
DOI: https://doi.org/10.21202/jdtl.2025.8

Уголовно-правовые проблемы противодействия преступности в метавселенной: современное состояние и перспективы развития

Марина Александровна Ефремова ✉

Российский государственный университет правосудия имени В. М. Лебедева, Москва, Россия

Евгений Александрович Русскевич

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), Москва, Россия

Ключевые слова

аватар,
виртуальность,
киберпреступность,
криминология,
метавселенная,
право,
преступность,
уголовная ответственность,
уголовное право,
цифровые технологии

Аннотация

Цель: исследование направлено на комплексный анализ уголовно-правовых рисков, возникающих в контексте развития метавселенной как нового цифрового пространства социального взаимодействия, определение понятия метавселенной и оценку возможностей противодействия преступной деятельности в данной среде средствами уголовного права.

Методы: методологию исследования составили диалектический метод научного познания, методы анализа и синтеза, а также совокупность специальных юридических методов. Применялся системный подход к изучению правовых явлений в цифровой среде, сравнительно-правовой метод для анализа зарубежного опыта, формально-юридический – для толкования нормативных актов и доктринальных положений.

Результаты: установлено, что привлекательность метавселенной для различных форм преступной деятельности в значительной степени обусловлена анонимностью пользователей и отсутствием четкого правового режима. Исследование показало, что на платформах метавселенной уже совершаются многочисленные преступления: общественно опасные деяния, связанные с распространением криминогенной и психотравмирующей информации, хищения цифрового имущества, преступная легализация доходов, посягательства против половой неприкосновенности личности. Выявлены системные проблемы противодействия преступности в метавселенной, включая территориальную юрисдикцию, идентификацию пользователей и процессуальные сложности доказывания.

✉ Корреспондирующий автор

Научная новизна: проведен комплексный анализ уголовно-правовых аспектов функционирования метавселенной. Сформулированы теоретические подходы к квалификации преступлений, совершаемых в виртуальном пространстве, обоснована необходимость разработки специальных правовых конструкций для регулирования отношений в метавселенной. Предложена концепция многомерной модели правовой охраны отношений в метавселенной, основанной на государственно-частном партнерстве.

Практическая значимость: результаты исследования могут быть использованы при совершенствовании уголовного законодательства в части регламентации ответственности за преступления, совершаемые в цифровом пространстве, разработке концепции правового регулирования метавселенной, создании механизмов государственно-частного партнерства в сфере противодействия киберпреступности. Полученные выводы актуальны для правоприменительной практики при расследовании преступлений, совершенных с использованием технологий виртуальной реальности.

Для цитирования

Ефремова, М. А., Русскевич, Е. А. (2025). Уголовно-правовые проблемы противодействия преступности в метавселенной: современное состояние и перспективы развития. *Journal of Digital Technologies and Law*, *3*(2), 187–202. https://doi.org/10.21202/jdtl.2025.8

Список литературы

Бегишев, И. Р., Денисович, В. В., Сабитов, Р. А., Пасс, А. А., Скоробогатов, А. В. (2023). Уголовно-правовое значение метавселенных: коллизии в праве. *Правопорядок: История, Теория, Практика*, *4*(39), 58–62. EDN: https://elibrary.ru/hehwgn. DOI: https://doi.org/10.47475/2311-696x-2023-39-4-58-62

Грибунов, О. П., Никонов, П. В., Пархоменко С. В., Рогова, Е. В. Шиханов, В. Н. (2023). *Цифровая валюта и цифровые финансовые права как предмет и средство совершения преступлений*. Иркутск: Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации. EDN: https://www.elibrary.ru/ryrwsj

Зайцев, О. А. (2024). Особенности уголовно-процессуального доказывания в условиях цифровизации. *Журнал российского права*, *8*, 93–112. EDN: https://elibrary.ru/bjnfvn. DOI: https://doi.org/10.61205/S160565900030639-6

Хабриева, Т. Я. (2018). Право перед вызовами цифровой реальности. *Журнал российского права*, *9*(261), 5–16. EDN: https://elibrary.ru/ozgiav. DOI: https://doi.org/10.12737/art_2018_9_1

Хаванова, И. А. (2024). Метавселенная: проблема адаптации налогово-правовых конструкций. *Журнал российского права*, *7*, 78–93. EDN: https://elibrary.ru/ejrgxj. DOI: https://doi.org/10.61205/S160565900029634-1

Alawadhi, I. M. (2023). *Future Cybercrimes in the Metaverse: A Comprehensive Forecast*. In H. Elshenraki (Ed.), Forecasting Cyber Crimes in the Age of the Metaverse (pp. 24–32). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-0220-0.ch002

AlMutawa, A., Ikuesan, R. A., & Said, H. (2024). Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model. *Future Internet*, *16*(12), 437. EDN: https://elibrary.ru/yoousp. DOI: https://doi.org/10.3390/fi16120437

AL-Tkhayneh, K. M., Olowoselu, A., & Alkrisheh, M. A. (2023). The Crime in Metaverse (the Future Scenarios for Crime Patterns and the Prospective Legal Challenges). In *2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), Abu Dhabi, United Arab Emirates* (pp. 1–6). https://doi.org/10.1109/snams60348.2023.10375402

Bhardwaj, A. (2024). *Cyber Fraud Use Cases in the Metaverse. In Beyond the Realms: Navigating the Metaverse* (pp. 106–130). Bentham science publishers. https://doi.org/10.2174/9789815238457124010007

Blake, J. (2024). Online Crime in the Metaverse: A Study on Classification, Prediction, and Mitigation Strategies. In H. N. Elshenraki (Ed.), *Forecasting Cyber Crimes in the Age of the Metaverse* (pp. 66–77). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch004

Chawki, M., Basu, S., & Choi, K.-S. (2024). Redefining Boundaries in the Metaverse: Navigating the Challenges of Virtual Harm and User Safety. *Laws*, *13*(3), 33. EDN: https://elibrary.ru/ssccdc. DOI: https://doi.org/10.3390/laws13030033

Cheong, B. C. (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, *3*, 467–494. EDN: https://elibrary.ru/bvvoth. DOI: https://doi.org/10.1365/s43439-022-00056-9

Duranske, B. T. (2008). *Virtual Law. Navigating the Legal Landscape of Virtual Worlds*. Chicago, Illinois: ABA Publishing, American Bar Association.

Fairfield, J. A. T. (2012). Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life. *Berkeley Technology Law Journal*, *27*, 55.

Gómez-Quintero, J., Johnson, Sh. D., Borrion, H., & Lundrigan, S. (2023). *A scoping study of crime facilitated by the metaverse*. https://doi.org/10.31235/osf.io/x9vbn

Lewandowsky, P. (2024). Cybercrime in the Meta-Universe. *Journal of Social Science and Humanities*, *6*(8), 5–8. EDN: https://elibrary.ru/kbjojn. DOI: https://doi.org/10.53469/jssh.2024.06(08).02

Lin, K.-X., Wu, J., Lin, D., & Zheng, Z. (2023). A Survey on Metaverse: Applications, Crimes and Governance. In *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom), Kyoto, Japan* (pp. 541–549). https://doi.org/10.1109/metacom57706.2023.00097

Marshall, A. M., & Tompsett, B. (2023). The metaverse – Not a new frontier for crime. *WIREs Forensic Science*, *6*(1), e1505. EDN: https://elibrary.ru/eilnzh. DOI: https://doi.org/10.1002/wfs2.1505

Mooij, A. (2024). *Regulating the Metaverse Economy*. Springer. https://doi.org/10.1007/978-3-031-46417-1

Narasimhan, P., & Kala, N. (2024). Securing the Metaverse: AI-Driven Solutions for Cyber Security, Privacy, and User Trust. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(6), 1890–1918. EDN: https://elibrary.ru/vakoem. DOI: https://doi.org/10.32628/cseit241061238

Qin, H. X., Wang, Y. & Hui, P. (2025). Identity, crimes, and law enforcement in the Metaverse. *Humanit Soc Sci Commun*, *12*, 194. https://doi.org/10.1057/s41599-024-04266-w

Saharan, S., Singh, S., Bhandari, A. K., & Yadav, B. (2024). The Future of Cyber-Crimes and Cyber War in the Metaverse. In H. N. Elshenraki (Ed.), *The Age of the Metaverse* (pp. 126–148). IGI Global. https://doi.org/10.4018/979-8-3693-0220-0.ch007

Singh, P. P. (2024). Cyber Crimes in Metaverse. *International Journal of Science and Research*, *13*(2). EDN: https://elibrary.ru/ulmpvh. DOI: https://doi.org/10.21275/mr24130195237

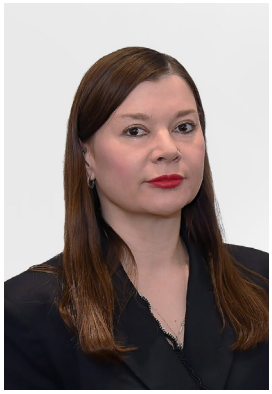
Teodorov, A.-V. (2023). Cybercrimes in the Metaverse: Challenges and Solutions. In *International Conference on Cybersecurity and Cybercrime*, 10 (pp. 209–215). https://doi.org/10.19107/cybercon.2023.28

Wasswa, S. (2023). Predicting Future Cybercrime Trends in the Metaverse Era. In H. N. Elshenraki (Ed.), *Forecasting Cyber Crimes in the Age of the Metaverse* (pp. 78–113). IGI Global. EDN: https://elibrary.ru/swgaya. DOI: https://doi.org/10.4018/979-8-3693-0220-0.ch005

Wiederhold, B. K. (2022). Sexual harassment in the metaverse. Cyberpsychology. *Behavior, and Social Networking, 25*(8), 479–480. EDN: https://elibrary.ru/hocuqv. DOI: https://doi.org/10.1089/cyber.2022.29253.editorial

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities. *IEEE Open Journal of the Computer Society*, *4*, 37–49. https://doi.org/10.1109/ojcs.2023.3245801

Сведения об авторах



Ефремова Марина Александровна – доктор юридических наук, профессор, заведующий кафедрой уголовно-правовых дисциплин Казанского филиала Российского государственного университета правосудия имени В. М. Лебедева
Адрес: 420088, Россия, г. Казань, ул. 2-я Азинская, 7а
E-mail: crimlaw16@gmail.com
ORCID ID: https://orcid.org/0000-0003-1076-2765
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57189299773
WoS Researcher ID: https://www.webofscience.com/wos/author/rid/E-6250-2016
Google Scholar ID: https://scholar.google.com/citations?user=mLPofnMAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=630526

Русскевич Евгений Александрович – доктор юридических наук, доцент, профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, 9
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
WoS Researcher ID: https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы являются членами редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 8 марта 2025 г.
Дата одобрения после рецензирования – 26 марта 2025 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.