World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-58, May-2026
ISSN: 2749-3601

VIRTUAL CRIMES AND ISSUES OF CRIMINAL LIABILITY IN THE DIGITAL AGE

Tolqinova Visola Ulugbek qizi
Tashkent State University of Law
Student of the Faculty of Criminal Justice
E-mail: visolatolqinova05@gmail.com

Article history:

Received: 24th March 2026
Accepted: 20th April 2026

Abstract:

This article analyzes the theoretical and practical problems of establishing criminal liability for crimes committed in virtual space. The subject of the research is criminal-law relations related to cyberbullying, online grooming, deepfake, avatar identification, virtual property and digital evidence. On the basis of comparative-legal, systemic, logical-legal and empirical methods, gaps in national legislation are identified and the need to introduce special elements of crimes, aggravating circumstances and procedural rules concerning digital evidence into the Criminal Code is substantiated. The results may be applied in adapting criminal legislation to the conditions of digital transformation, improving judicial and investigative practice, effectively protecting victims and developing prevention policy.

Keywords: Virtual space, cybercrime, criminal liability, cyberbullying, online grooming, deepfake, avatar identification, digital evidence.

INTRODUCTION

As a result of digital transformation, the classical forms of crime are moving into the virtual environment and are raising new questions for criminal-law theory and lawmaking. The Internet, social networks, cloud infrastructures, crypto-assets, metaverse platforms and artificial intelligence tools, on the one hand, expand a person's opportunities to exchange information, conduct economic activity and express creative identity, while, on the other hand, they generate new socially dangerous acts against the interests of the individual, society and the state. Therefore, it is theoretically and practically insufficient to limit crimes in virtual space only to unauthorized access to an information system or the distribution of malicious software. Virtual space must be assessed comprehensively as an environment where a crime is committed, a means of committing a crime, a field where the consequences of a crime appear and an information space where digital evidence is formed.

The relevance of the topic is also directly connected with the development of national legislation. Reforms carried out in the Republic of Uzbekistan to develop the digital economy and digitalize public services, in particular, the Decree of the President of the Republic of Uzbekistan No. PF-6079 of October 5, 2020, "On approval of the Digital Uzbekistan - 2030 Strategy and measures for its effective implementation", have turned the provision of information security into an important area of state policy. The Law of the Republic of Uzbekistan "On Cybersecurity" of April 15, 2022, defines the principles of ensuring cybersecurity and the system of authorized entities. At the same time, the Decree of the President of the Republic of Uzbekistan No. PF-33 "On additional organizational and legal measures to strengthen the protection of the rights of women and children and to prevent cases of harassment and violence against them", which is aimed at protecting the rights of women and children, sets the task of establishing strict liability for cyberviolence and online grooming committed on the Internet or social networks. This shows that the issue has risen to the level of a practical necessity.

The purpose of the article is to identify the existing theoretical and legal gaps in the criminal legislation of the Republic of Uzbekistan regarding the establishment of liability for crimes in virtual space and the qualification of acts, to compare them with international standards and foreign experience, and to develop scientifically substantiated proposals for improving legislation. To achieve this purpose, the boundaries of the concepts of virtual space and cybercrime are clarified; virtual space is analyzed as a method and means of committing a crime; the features of determining the elements of a crime in the digital environment are explained; the coverage in national law of acts related to cyberbullying, online grooming, deepfake, avatar identification and virtual property is assessed; and criminal-procedural approaches to digital evidence and jurisdictional problems are substantiated.

In national scientific literature, M.X. Rustambayev formed the theoretical foundation for crimes in the field of information technologies by commenting on the norms of the Special Part of the Criminal Code[1]. S.S. Niyozova studied the concept of cybercrime, information security and the prevention of

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-58, May-2026
ISSN: 2749-3601

digital acts, in particular, pointing out as a practical problem the absence of a special norm covering intentional and systematic acts of harassment against a person through electronic means of communication[2]. A. Khalmuratov, analyzing the adaptive model of liability for digital crimes and the adaptation of criminal legislation to new technological threats, specifically emphasized that it is impossible to fully qualify cyberbullying acts within the current articles on defamation, insult and threat, which creates a gap in criminal liability[3]. In foreign sources, F.G. Lastowka and D. Hunter examined the legal status of virtual persons and virtual objects[4], J. Grimmelmann studied the governance of virtual worlds and the problems of virtual property[5], while J. Fairfield substantiated the proprietary legal nature of virtual property[6]. A. Karapatakis comparatively analyzed fraud and sexual offences in the metaverse using the example of English law[7]. INTERPOL's 2024 white paper systematized metaverse crimes from the perspective of law enforcement[8].

Although the existing studies have created an important theoretical basis, crimes committed in virtual space have not yet been sufficiently developed in the science of criminal law of Uzbekistan as a separate, independent and complex category. In the Republic of Uzbekistan, cybercrimes have increased 68 times over the last five years, and in 2024 alone they increased 9.1 times compared with 2023. Crimes in the field of information technologies account for 50 percent of all crimes. The number of citizens' appeals concerning violations in cyberspace has increased 34 times[9]. Today, the scope of digital space is expanding at an unprecedented pace: the number of users, which was 4.66 billion in 2020, reached 4.95 billion by the beginning of 2022. The World Economic Forum's 2023 report recognized cybercrime as one of the ten most dangerous global threats and forecast that global damage will reach 10.5 trillion dollars by 2025[10].

Therefore, no uniform approach has been formed in national doctrine regarding the features of cyberbullying as an independent element of a crime, the special element of online exploitation of minors, the criminal-law assessment of deepfake content created with the help of artificial intelligence, avatar identification and the protection of virtual property, the procedural status of digital evidence and issues of transboundary jurisdiction. This article is aimed at filling that gap.

MAIN PART

The object of the research is the set of social relations arising in the process of establishing criminal liability for crimes committed in virtual space. The subject of the research consists of the Criminal Code of the Republic of Uzbekistan, the Criminal Procedure Code, the Law "On Cybersecurity", the Budapest Convention, the UN Convention against Cybercrime, the European Union Regulation on Artificial Intelligence[11], the experience of the United Kingdom[12], Australia, Singapore, the Republic of Korea and other states, as well as scientific literature and the results of an empirical survey.

The article uses comparative-legal, systemic, logical-legal, formal-legal, empirical and modeling methods. The comparative-legal method made it possible to compare national legislation with the Budapest Convention, the UN Convention, the EU AI Act[13], the Online Safety Act 2023, the Sexual Offences Act 2003 and other foreign instruments. The systemic method served to assess acts in virtual space not only by separating them into individual articles, but also together with the elements of a crime, victim protection, the role of platforms, digital evidence and jurisdictional elements. The formal-legal method was used to determine the possibilities and limits of qualifying acts under the current articles. The empirical method showed the subjective perception of the social danger of virtual crimes through the analysis of the results of an indicative survey conducted among TSUL students.

First of all, it is necessary to define the concept of a "crime in virtual space". In the classical sense, cybercrime means acts committed by means of, against or with the help of an information system or computer network. However, crimes in virtual space are a broader concept. They may harm social relations formed in the digital environment, a person's virtual identity, digital property, psychological inviolability, children's safety and public order. In this sense, virtual space is not only a technical platform for committing a crime, but also determines the socio-legal content of the result of the crime.

The *first feature* distinguishing crimes in virtual space from cybercrime is immersiveness. On metaverse or virtual reality platforms, a user acts through an avatar, communicates with other persons, possesses virtual objects and disposes of digital assets that have certain economic value. The *second feature* is multi-layered identification: one person may act through several avatars, accounts or crypto-wallets, while, conversely, one avatar may be controlled by several persons. The *third feature* is transboundary nature: the offender, the victim, the server, the payment infrastructure and the harmful consequence may be located in different jurisdictions. The *fourth feature* is that evidence is formed in the form of digital traces.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-58, May-2026
ISSN: 2749-3601

The criminological features of crimes in virtual space are as follows. Geographical borderlessness: even if a crime is committed in one country, its consequences may spread throughout the world. At the same time, because misappropriated funds are withdrawn in the form of crypto-assets, fully detecting the crime and compensating material damage becomes complicated. The next feature is anonymity: the offender hides his or her true identity through digital avatars, VPNs or other technical means. In the metaverse, committing a crime first requires immersion in the virtual environment by means of special equipment, which constitutes an important difference from classical cybercrime.

According to a study by the World Economic Forum, in 83 percent of blockchain-based crimes, the possibility of bringing offenders to criminal liability is limited because of technical and legal obstacles. For this reason, determining the "place of commission" of a crime in virtual space is much more complicated than in traditional cybercrime[14]

When virtual space is assessed as a method of committing a crime, attention is paid to the system of actions chosen by the offender to achieve the goal. Phishing, social engineering, distribution of malicious software, DDoS attacks, ransomware, deception through deepfake, sextortion, cyberbullying, online grooming, seizure of avatar identification or unauthorized entry into a virtual area are among such methods. As a means of crime, a website, botnet, malicious software, VPN, Tor network, dark web platform, artificial intelligence generator, crypto-wallet, virtual reality device or digital platform may be used. In the digital environment, the means and the method often become inseparable: deepfake technology is simultaneously a means of crime and a method of misleading the victim.

Chapter XX¹ of the Criminal Code of the Republic of Uzbekistan establishes liability for crimes in the field of information technologies. This chapter covers such acts as violation of informatization rules, unlawful use of computer information, unauthorized access to a computer system, and creation and distribution of malicious programs. However, the current model of this chapter is mainly directed at acts against the confidentiality, integrity and functioning of computer data, systems and networks. New threats in virtual space often harm a person's psychological inviolability, honor and dignity, sexual freedom, children's safety, virtual assets and the reliability of information. Therefore, Chapter XX¹ of the Criminal Code is not sufficient to fully cover all acts in virtual space.

First, cyberbullying has not been established as an independent element of a crime. In practice, cyberbullying may often be assessed within separate norms such as insult, defamation, violation of privacy, threat of murder or use of violence. However, the social danger of cyberbullying is manifested precisely in its repetitive nature, its rapid spread to a broad audience in the digital environment, the victim's remaining under constant psychological pressure and the long-term preservation of digital traces. Therefore, it differs from a single insult or an ordinary threat. According to the World Health Organization's 2024 international report, cyberbullying among young people and adolescents is increasing at a dangerous level: from 2018 to 2022, the rate of becoming a victim of cyberbullying increased from 12 percent to 15 percent among boys and from 13 percent to 16 percent among girls. Overall, currently on average one out of every six adolescents (15%) is subjected to harassment and violence in digital space. This growth dynamic confirms at the international level how urgent it is to establish strict and special criminal liability for acts of cyberviolence in national criminal legislation[15]. On this basis, first of all, the following term should be added to Section Eight of the Criminal Code. **The need to introduce a special norm for cyberbullying is substantiated by three criteria.** First, the object of this act is not only honor and dignity, but also the person's psychological inviolability, information security and freedom in digital social relations. Second, the objective side appears through repeated, systematic or mass digital influence; this may include harassment through comments, posts, videos, images, edits, memes and bots, disclosure of personal data or forcing the victim into social isolation. Third, on the subjective side, there is intent to humiliate, intimidate, inflict mental suffering on or discredit the victim. If these features are not expressed in the form of a separate article, judicial and investigative practice may underestimate the true social danger of the act.

Second, the special element of a crime concerning online grooming and digital exploitation of minors has not been sufficiently developed. **Online grooming** consists of step-by-step actions aimed at establishing a relationship of trust with a minor through the Internet, psychologically preparing the minor and subsequently subjecting him or her to sexual exploitation. In traditional elements of crimes, harm is often assessed after physical contact or a specific fact of exploitation. In the virtual environment, however, the danger arises earlier, at the stage of establishing contact, gaining trust, requesting intimate images, inducing a meeting or forcing the child to create self-exposing content. The presence in the United Kingdom

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-58, May-2026
ISSN: 2749-3601

Sexual Offences Act 2003 of a special approach to preparing a child for sexual purposes through online communication has comparative significance for national legislation[16].

Third, there is the criminal-law assessment of the use of deepfake and artificial intelligence. A deepfake creates fake content that appears credible by artificially creating or modifying a person's voice, appearance or actions. Such content may be a means of fraud, extortion, discrediting, preparing pornographic material, interfering with the electoral process, falsifying evidence or violating privacy. The European Parliament and Council AI Act attempted to regulate deepfake threats by restricting the dangerous use of artificial intelligence and establishing transparency obligations concerning synthetic content[17]. In criminal law, however, deepfake may not always be assessed as a separate crime, but also as a means or aggravating circumstance that increases the level of social danger of a particular act. **A three-stage approach to deepfake is appropriate.** The first stage is to criminalize the creation and distribution of non-consensual intimate deepfake as an encroachment on private life and sexual inviolability. The second stage is to establish the use of deepfake as an aggravating circumstance when fraud, extortion, defamation, interference with the electoral process or falsification of evidence is committed through deepfake. The third stage is to regulate in separate legislation the obligations of platforms and service providers to label synthetic content, review complaints and promptly restrict illegal content. Such a model is consistent with the principle of subsidiarity in criminal law, because not every deepfake content is automatically a crime, but criminal liability is justified when it causes socially dangerous harm to a person, society or the state.

Fourth, there is the protection of avatar identification and virtual property. An avatar is a user's digital representative in the virtual environment through which a person communicates, carries out economic operations and participates in digital communities. The seizure of avatar identification makes it possible to act on behalf of a person, damage that person's reputation, misappropriate virtual assets or mislead other persons. Virtual property may acquire economic value in the form of an NFT, an in-game item, an avatar accessory, a virtual land plot, a digital art object or an in-platform token. Fairfield describes virtual property as an object that, although digital, has real value for the user[18]. Grimmelmann points to the complexity of the balance of powers among the platform owner, the user and the state in virtual worlds[19]

The current criminal legislation does not always clearly and fully cover virtual property as traditional "property". This is because many articles are based on the concept of possessing, destroying or damaging a tangible object. A virtual asset may be connected with a record in a database, a token, a contractual right or the internal rules of a platform. Therefore, when assessing the unlawful possession, damage or use of a virtual asset from a criminal-law perspective, the criteria of economic value, the user's legitimate control, platform terms and real harm caused to the victim must be taken into account.

In addition, the fact that the cost of copying and distributing digital tools is almost zero significantly increases their level of social danger. As substantiated in A. Khalmuratov's research, the concept of "violation of informatization rules" in current Article 278¹ of the Criminal Code does not fully cover all forms of these methods, such as phishing, ransomware, DDoS, sextortion, cyberbullying, theft of avatar identification and artificial-intelligence-based attacks[20]

South Korea, through the Virtual Asset User Protection Act (VAUPA), which entered into force on July 19, 2024, recognized virtual assets as an independent object of crime and introduced a two-tier system of sanctions for price manipulation, use of inside information and fraud[21]. This model deserves special attention: without equating virtual property with traditional theft, it makes it possible to establish separate qualification criteria. This approach may serve as a methodological guide in resolving certain problems arising in the application of Articles 169 and 278² of the Criminal Code.

The articles of the German Federal Criminal Code, namely Articles 202a, 263a, 303a and 303b, are drafted in a technologically neutral manner: they do not name a specific technology, but define the elements through broad expressions such as unlawful conduct in relation to data[22]. This approach ensures that when new technologies such as artificial intelligence, blockchain and the metaverse appear, the norms retain their force. The articles of Chapter XX¹ of the Criminal Code of Uzbekistan, however, are currently strongly tied to the concepts of "computer" and "information system", which makes adaptation to future new technologies difficult.

The United Kingdom's Computer Misuse Act 1990 and Online Safety Act 2023 have formed a unified system covering not only technical cyberattacks, but also harmful online content and acts against persons in the virtual environment. The first investigation of sexual assault in a virtual environment opened in the United Kingdom in 2024 was qualified precisely within

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-58, May-2026
ISSN: 2749-3601

this complex regulatory framework[23]. In the United States, although the Computer Fraud and Abuse Act was adopted in 1986, it is gradually being adapted through judicial practice to virtual property and metaverse crimes.

Fifth, there is the procedural status of digital evidence. Crimes in virtual space are often proved through log files, IP addresses, traffic data, blockchain transactions, server records, screenshots, audio-video content, metadata and internal platform correspondence. The specific nature of digital evidence is that it changes quickly, is easily deleted, when copied loses the distinction between the original and the copy, and is often stored on transboundary servers. Therefore, clear rules must be established for its acquisition, preservation, examination and assessment in court, including chain of custody, hash values, metadata integrity, procedural authorization by the competent entity and mechanisms of cooperation with platforms. **The Budapest Convention** serves as an important model for working with digital evidence by establishing mechanisms for the expedited preservation of computer data, the preservation and disclosure of traffic data, the search of computer systems and international cooperation. The UN Convention against Cybercrime adopted in 2024 regulates even more broadly the exchange of evidence in electronic form and cooperation against transboundary crimes. The introduction of a separate chapter or special rules on digital evidence into the criminal-procedural legislation of Uzbekistan would increase the stability of investigative practice[24]

Sixth, there is the issue of jurisdiction. When a crime is committed in virtual space, the place of the act, the place of the consequence, the state where the victim is located, the state where the server is located, the state where the platform is registered and the offender's actual location may all differ. The traditional principle of territoriality is not sufficient in such situations. Therefore, in determining jurisdiction over virtual crimes, a multi-factor model should be applied: the consequence of the act in the territory of Uzbekistan, the fact that the victim is a citizen or resident of Uzbekistan, damage to national information systems, the offender's action in the territory of Uzbekistan or the connection of the benefit obtained as a result of the crime with Uzbekistan should be taken into account. Such an approach restricts offenders from avoiding liability by abusing the location of the server or platform. **Foreign experience** shows that two main models are emerging in the regulation of crimes in virtual space. The first model is based on technological neutrality: an aggravating circumstance such as "committed using telecommunication networks or the global Internet information network" is added to existing elements of crimes. This model is rapid and preserves codification stability, but does not always reveal the specific social danger of new acts. The second model is based on creating special elements: acts such as cyberbullying, online grooming, distribution of non-consensual intimate images, intimate deepfake content and encroachments on virtual assets are defined as separate norms. This model is more precise, but may create a risk of excessive criminalization. For Uzbekistan, the optimal solution is a mixed model: acts with independent social danger such as cyberbullying and online grooming should be established as separate elements, while the use of deepfake and artificial intelligence should be established as an aggravating circumstance for certain crimes.

Empirical indicators also confirm the need to improve national legislation. Within the graduation research, an indicative survey conducted among TSUL students shows that crimes in virtual space are not merely a theoretical assumption, but are perceived by young people as a real threat. 66.7 percent of respondents stated that they use the Internet and social networks for several hours every day, 44.4 percent stated that they had encountered fraud, threats or deception in virtual space, and 88.9 percent stated that cybercrimes have increased greatly in recent years. In particular, the fact that 100 percent of respondents indicated the need for separate liability for cyberbullying clearly demonstrates the gap between social demand and legal deficiency.

Legal interpretation of the results of the indicative survey among TSUL students

Indicator	Result	Criminal-law interpretation
Activity of using the Internet and social networks	**66.7% - several hours every day; 33.3% - 1-2 hours per day**	**Shows that virtual space is a permanent element of students' daily life.**
Encountering fraud, threats or deception	**44.4% - yes; 55.6% - no**	**Virtual crimes are manifested as a real risk of victimization.**

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-58, May-2026
ISSN: 2749-3601

Assessment of cybercrime dynamics	**88.9% - increased greatly; 11.1% - increased slightly**	**Respondents perceive the growth of digital threats at a high level.**
The most dangerous virtual crimes	**66.7% - online fraud; 22.2% - deepfakes and fake videos; 11.1% - crimes against children**	**Along with online fraud, deepfake and children's safety require special attention.**
Sufficiency of current legislation	**75% - insufficient; 12.5% - partially sufficient; 12.5% - sufficient**	**The scientific conclusion about a legal gap is supported by the respondents' position.**
Need for separate liability for cyberbullying	**100% - yes**	**Establishing cyberbullying as an independent element of a crime is socially justified.**
Concern about personal data security	**66.7% - very concerned; 33.3% - not very concerned**	**The inviolability of personal data is a central element of preventing virtual crimes.**

The survey results do not claim statistical representativeness, but they are an important indicative source for identifying the social sensitivity of the legal problem. In particular, the fact that the majority of respondents assessed the current legislation as insufficient and that all of them indicated the need for separate liability for cyberbullying confirms the necessity of harmonizing preventive and repressive mechanisms in criminal legislation. In this sense, the empirical indicators correspond to the theoretical analysis: crimes in virtual space do not harm only technical systems, but directly encroach upon the person's psychological security, honor, dignity, property interests and the inviolability of children.

On the basis of the analyses conducted during the research, the following scientifically substantiated proposals aimed at adapting the criminal legislation of the Republic of Uzbekistan to new types of crimes in virtual space were developed.

First, it is proposed to introduce the author's definitions of the concepts of "cyberviolence" and "artificial intelligence technologies" into Section Eight, "Terms", of the Criminal Code. As S.S. Niyozova and other scholars emphasize, the absence of clear legal definitions in legislation leads in practice to different interpretations and qualification errors. In this regard, **"cyberviolence" (cyberbullying)** should be defined as a set of acts committed intentionally and systematically against a person through electronic means of communication, information and communication technologies, social networks or digital platforms, which cause psychological harm, fear, mental suffering or a decline in quality of life, and which take the form of placing the person in social isolation, humiliating or discrediting him or her. **"Artificial intelligence technologies"** should be defined as software and hardware complexes and artificial neural networks capable of imitating human cognitive functions, including creating and analyzing text, images and sound, and performing certain tasks autonomously or partially autonomously.

Second, it is necessary to introduce Article 112¹ entitled "Cyberviolence" into the Criminal Code: this article would define as a crime the severe impact on a person's psyche through intentional and systematic harassment by means of telecommunication networks, sending materials containing threats or insults, creating and using a fake virtual identity in the person's name, and disseminating information about the person without his or her consent; if committed against minors or by a group, imprisonment for three to five years would be provided. As substantiated in the studies of A. Khalmuratov and S.S. Niyozova, the current articles on defamation, insult and threats do not cover important features of cyberviolence such as systematic nature, psychological harm and the creation of a fake virtual identity, which creates a gap in criminal liability

Third, it is proposed to introduce subparagraph "v" into part four of Article 131 of the Criminal Code and subparagraph "l" into part two of Article 135 with the content "if committed using telecommunication networks or the global Internet information network".

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-58, May-2026
ISSN: 2749-3601

This proposal is substantiated by the fact that, as noted in INTERPOL's 2023 report, crimes against children in the digital environment have increased by 87 percent over the last five years, while in foreign experience, namely the United Kingdom Sexual Offences Act 2003 and the Australian Criminal Code Act 1995, grooming is included in the existing section on sexual offences.

Fourth, based on the principle of legality and the requirements of internal consistency of the elements of crimes substantiated by M.X. Rustambayev, it is proposed to introduce into Articles 130, 130¹, 139, 140, 141¹, 141², 141³, 158, 165, 209, 228 and 244⁶ of the Criminal Code a single aggravating subparagraph with the content *"if the same acts are committed using a fake image, video or audio material created with the help of artificial intelligence technologies or special algorithms"*.

CONCLUSION

This study substantiated the institution of criminal liability for crimes in virtual space as an independent scientific and practical problem in the criminal law of Uzbekistan. The results of the analysis showed that although the current Chapter XX¹ of the Criminal Code (Articles 278¹-278⁷) partially regulates technical acts against information systems, it does not fully cover, from the standpoint of criminal liability, new types of acts such as cyberbullying, online grooming, crimes based on deepfake technology, theft of avatar identification and damage to virtual property. In order to eliminate the gaps identified during this scientific research, a mixed normative model was proposed. Under the first direction, taking into account the need to establish acts with independent social danger, such as cyberbullying and online grooming, as separate elements of crimes, it is proposed to introduce Article 112¹, "Cyberviolence", into the Criminal Code and to add to Articles 131 and 135 an aggravating subparagraph covering commission through telecommunication networks. Under the second direction, the use of deepfake and artificial intelligence technologies should be introduced as an aggravating circumstance into Articles 130, 139, 140, 141¹, 141², 141³, 165 and twelve other articles. Under the third direction, it was analyzed that special norms regulating the procedural status of virtual assets, avatar identification and digital evidence should be introduced into the Criminal Procedure Code, and that without clear rules defining the procedural status of digital evidence, proving a crime in virtual space in court becomes almost impossible.

The proposed normative proposals fully preserve the ultima ratio nature of criminal law, that is, the principle that criminalization should be applied only to intentional acts with significant social danger, and were formed in accordance with the requirements of the Budapest Convention, the UN Convention against Cybercrime of 2024 and the "Digital Uzbekistan - 2030" Strategy of the Republic of Uzbekistan. Thus, the institution of liability for crimes in virtual space should be developed not only as a punitive mechanism, but also as a complex legal mechanism serving to protect victims, ensure children's safety and strengthen the stability of national cyberspace.

REFERENCES

1. Rustambayev, M. X. (2024). Commentary to the Criminal Code of the Republic of Uzbekistan: Special Part. Tashkent: Adolat.
2. Niyozova, S. S. (2021). Cybercrime. Tashkent: Tashkent State University of Law Publishing House.
3. Lastowka, F. G., & Hunter, D. (2004). The laws of the virtual worlds. California Law Review, 92(1), 1-74;
4. Khalmuratov. Criminal-legal transformation of combating cybercrime in the Republic of Uzbekistan: the concept of adaptive punishment and digital law enforcement // Society and Innovations. - 2025. https://doi.org/10.47689/2181-1415-vol6-iss12/S-pp224-233
5. Grimmelmann, J. (2006). Virtual world governance. Yale Journal of Law & Technology, 8, 1-75.
6. Fairfield, J. A. T. (2005). Virtual property. Boston University Law Review, 85, 1047-1102;
7. Karapatakis, A. (2025). Metaverse crimes in virtual (Un)reality: Fraud and sexual offences under English law. Journal of Economic Criminology, 7, 100070. https://doi.org/10.1016/j.jeconc.2024.100070
8. INTERPOL. Metaverse: A Law Enforcement Perspective: Use Cases, Crime, Forensics, Investigation and Governance.
9. https://www.gazeta.uz/ru/2025/11/06/cybersecurity/
10. World Economic Forum. The Global Risks Report 2023. 18th Edition. Geneva: WEF, 2023. pp. 14-17. URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
11. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-58, May-2026
ISSN: 2749-3601

12. United Nations General Assembly. (2024). United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes. United Nations.
13. European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union.
14. World Economic Forum. Global Risks Report 2023. Geneva: WEF, 2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf https://www.weforum.org/reports/global-risks-report-2023.
15. Canada. Bill C-13, 2014; Singapore. Protection from Harassment Act 2014, ss. 3-4; Australia. Online Safety Act 2021 (Cth), ss. 36-40; UK. Online Safety Act 2023, s. 5.
16. The Parliament of the United Kingdom. (2003). Sexual Offences Act 2003. https://www.legislation.gov.uk
17. European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union. https://eur-lex.europa.eu
18. Lehdonvirta, V. (2009). Virtual item sales as a revenue model: Identifying attributes that drive purchase decisions. Electronic Commerce Research, 9, 97-113. https://doi.org/10.1007/s10660-009-9028-2;
19. Strikwerda, L. (2012). Theft of virtual items in online multiplayer computer games: An ontological and moral analysis. Ethics and Information Technology, 14, 89-97. https://doi.org/10.1007/s10676-011-9285-3
    A. Khalmuratov. Criminal-legal transformation of combating cybercrime in the Republic of Uzbekistan // Journal of Law. - 2025. - No. 2. - p.
20. Korea Financial Services Commission. Virtual Asset User Protection Act. URL: https://www.fsc.go.kr/eng/index
21. Hilgendorf E. Computerstrafrecht in Zeiten des Metaverse // Neue Juristische Wochenschrift.
22. Computer Misuse Act 1990 (UK), ss. 1-3A; Online Safety Act 2023, Part 10
23. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185), arts. 16-21. https://www.coe.int