

PROTECTING WOMEN'S RIGHTS IN THE DIGITAL SPACE: LEGAL MECHANISMS AGAINST CYBER VIOLENCE**Toshmamatova Shakhrizoda Dilmurod qizi**3rd year student of the direction of "Jurisprudence"
Karakalpak State University named after Berdaq

Abstract. This article is dedicated to the study of protecting women's rights in the digital space and effective legal mechanisms against cyber violence. The article pays particular attention to risks emerging in the online environment as a result of the development of modern information and communication technologies, including sexual discrimination, threats, harassment, and cyberattacks. Moreover, the article analyzes practical legal mechanisms in Uzbekistan and foreign countries, including laws, regulatory documents, and international standards. The findings of the article indicate that effective monitoring, preventive measures, and the development of online reporting systems can reduce cyber violence against women.

Keywords: digital space, women's rights, cyber violence, legal mechanisms, online protection, sexual discrimination.

Introduction.

The digital space has become an integral part of people's daily lives and social interactions. The Internet, social networks, and various digital platforms are not only means of accessing and sharing information but also essential tools for work, education, commerce, and other social processes. At the same time, the digital space has contributed to the widespread occurrence of cyber violence against women. Cyber violence refers to phenomena in the online environment that include threats, harassment, sexual discrimination, intrusion into private life, and other harmful actions. Women are particularly at high risk of such attacks, as their personal data, photos, and videos can be misused or distributed without consent.

The legislation of the Republic of Uzbekistan pays special attention to the protection of women's rights in the digital space. In particular, Article 46 of the Constitution of Uzbekistan emphasizes that all citizens, regardless of gender, have equal rights [1] and prohibits discrimination against women. Additionally, the Law "On Ensuring Equal Rights of Women and Men" guarantees women's social, political, economic, and cultural rights and provides a legal basis for applying protection mechanisms in cases of cyber violence.

To reduce cyber violence and create a safe environment in the digital space, Uzbekistan has established mechanisms for ensuring information security, protecting personal data, and detecting crimes online through laws such as the "On Informatization" Law [2] and the "On Electronic Commerce" Law [3]. These laws not only strengthen cybersecurity but also enable the protection of women's rights on digital platforms. For instance, it is explicitly stated that legal measures can be taken if personal data or photographs are distributed without permission.

Foreign experiences also demonstrate effective mechanisms for protecting women's rights in the digital space. Recommendations from the European Union and the United Nations, including the UN's Guidelines on Combating Cyber Violence Against Women [4], emphasize prompt action in cases of online harassment and threats, protection of personal data, and raising awareness. Based on this, harmonizing Uzbekistan's current legislation with international standards can ensure the protection of women's rights in the digital environment.

The article also analyzes various forms of cyber violence, including online stalking, threatening messages, dissemination of sexually explicit content, and illegal use of personal data. To enhance the effectiveness of legal mechanisms against cyber violence, it is essential to have a strong legal framework, relevant monitoring systems, and prompt judicial and law enforcement measures.

Additionally, to reduce cyber violence against women, it is important to strengthen preventive and educational measures in the field of information and communication technologies. For example, organizing training on improving digital literacy, using secure passwords, protecting personal data, and identifying dangerous content online can be highly beneficial.

Research Methodology.

In this article, both qualitative and quantitative research methods were combined to analyze cyber violence against women in the digital space. The primary data were collected through online surveys, interviews, and social media monitoring. Statistical analysis was used to identify various forms of cyber violence and their prevalence, as well as to assess their psychological and social impact. Additionally, the study involved a review of previous research and international experiences, which allowed for comparative analysis of the findings. Data processing and analysis employed graphical and tabular methods to present the results clearly and comprehensibly. Special attention was given to developing practical recommendations for preventing cyber violence during the research process.

Analysis and Results.

Analysis of various forms of cyber violence against women in the digital space clearly demonstrates both its widespread prevalence and significant social harm. According to recent national and international statistics, cases of online threats, unauthorized dissemination of personal information, and sexually abusive behavior have sharply increased in recent years. For instance, the 2024 report of the Ministry of Internal Affairs of the Republic of Uzbekistan recorded a total of 3,500 cybercrime incidents, 42% of which involved women [5]. These figures highlight the seriousness of security issues in the digital space.

One of the main forms of cyber violence is online stalking, where a woman's social media profiles, personal photos, or videos are monitored without consent, violating her privacy. Studies indicate that more than 60% of online stalking incidents occur on social media platforms. In response, Article 139 of the Criminal Code of the Republic of Uzbekistan ("Violation of Privacy") [6] and the Law on "Informatization" establish mechanisms for identifying and punishing cybercrimes.

Another significant form of cyber violence is the dissemination of threatening and abusive messages. These incidents are particularly widespread on social media and have severe negative effects on women's mental health. International experience shows that in European Union countries, cases of online threats against women increased by 35% in 2023. Based on this, the UN's "Guidelines on Combating Cyber Violence Against Women" recommend rapid reporting mechanisms and strengthened preventive measures.

In Uzbekistan, prompt monitoring and the awareness of law enforcement agencies have led to the identification of numerous cases, with offenders being held administratively or criminally responsible. Unauthorized dissemination of personal information and the creation of sexually explicit content remain serious concerns. According to statistics, in 2024 there were 1,470 recorded cases related to online content harming women. To prevent such incidents, Uzbekistan has established mechanisms for protecting personal information under the "Informatization" Law and the "Electronic Commerce" Law. For example, if a photo or video is distributed without consent, the victim can promptly file a complaint, after which the relevant authorities block the content and hold the offender accountable.

The analysis results indicate that effective legal mechanisms, particularly laws, monitoring systems, and rapid response measures, play a crucial role in reducing cyber violence. However, their effectiveness is closely linked to the level of digital literacy and social awareness. For instance, many women are not sufficiently aware of online security measures, which exposes them to potential threats. Therefore, to create a safe environment in the digital space, it is necessary not only to strengthen legal mechanisms but also to enhance users' knowledge through education and training programs.

International experience also demonstrates that the most effective way to combat cyber violence is to harmonize legislation with international standards and develop monitoring systems on online platforms. For example, in Europe and the United States, there are specialized laws for personal data protection and rapid response services. Based on this, Uzbekistan is also reinforcing existing laws and implementing effective mechanisms to strengthen cybersecurity.

As a result, the analysis identifies the following key measures to reduce cyber violence against women in the digital space:

1. Enhancing the effectiveness of legal mechanisms, i.e., improving laws and regulatory documents;
2. Developing online monitoring and rapid response systems;
3. Increasing digital literacy and strengthening education on security measures;
4. Applying international standards and experiences – identified as the most important measures.

Thus, the results of this study confirm the effectiveness of legal mechanisms in protecting women's rights and reducing cyber violence in the digital space and can serve as a basis for developing practical measures.

Discussion.

The prevalence of cyber violence against women in the digital space is not only an individual concern but also a significant social issue. The analysis results indicate that threats, harassment, and unauthorized dissemination of personal information occur frequently in online environments. Such situations negatively affect women's mental health, social engagement, and professional activities, limiting their ability to protect themselves in the digital space.

Recent statistical studies, particularly those conducted in 2023–2024 on online platforms, show that the most common forms of cyber violence against women include threatening messages on social media, unauthorized distribution of personal photos and videos, and offensive or harmful comments. Moreover, cybercrimes not only endanger individual users but also pose risks to entire online communities. This undermines social trust in the digital environment and hinders women's effective use of internet resources.

The discussion highlights that enhancing digital literacy and technological security are among the most critical factors in reducing cyber violence. For instance, if users are informed about using secure passwords, sharing personal information with limited audiences, and identifying online threats, the likelihood of cybercrimes decreases significantly. Additionally, social awareness campaigns and educational programs alert users to the various forms of cyber violence and provide guidance on protective measures.

Technological solutions also play a crucial role in effectively combating cyber violence. AI-based monitoring systems, automated spam filters, and tools for detecting harmful content help reduce online threats. Such systems allow users to communicate safely, while potential threats are promptly identified and neutralized. Furthermore, expanding reporting and support mechanisms on platforms enhances the effectiveness of anti-cyber violence measures. Overall, the discussion demonstrates that protecting women's rights and reducing cyber violence in the digital space depends not only on technological solutions and user awareness but also on social, cultural, and psychological factors. For example, fostering a culture of respect and safety online and creating peer support systems among users also contribute to reducing cybercrimes.

Conclusion and Recommendations.

The prevalence of cyber violence against women in the digital space, as revealed by the analysis and discussion, represents the intersection of global and local challenges. Cyber violence threatens not only personal safety but also mental health and social engagement. Analyses indicate that women frequently face issues such as threats, harassment, and unauthorized dissemination of personal information on social media and online platforms. These

situations significantly affect their use of digital environments and limit their ability to protect themselves.

In conclusion, protecting women's rights and reducing cyber violence in the digital space is a long-term process that cannot rely solely on technological solutions. Raising social awareness and fostering a culture of online respect and safety are equally important. Additionally, enhancing users' personal experience and knowledge of digital security contributes to safer online environments.

The following recommendations are proposed:

1. Organize comprehensive educational and training programs on digital security, particularly aimed at raising awareness among women about threats and cyber violence.
2. Develop monitoring and rapid response systems on online platforms to protect users.
3. Strengthen social awareness campaigns and foster a culture of respect and safety among users.
4. Implement a multidisciplinary approach to reduce the psychological, social, and economic harm caused by cyber violence.
5. Expand technological solutions for protecting users' personal data and detecting harmful content.

If these measures are implemented, the digital space can become a safer and more equitable environment for women, and efforts to prevent cyber violence can achieve effective results. This will have positive implications not only for individual users but also for society as a whole.

References:

1. O'zbekiston Respublikasi Konstitutsiyasi 01.05.2023. <https://lex.uz/uz/docs/-6445145>
2. O'zbekiston Respublikasining qonuni, 11.12.2003 yildagi 560-II-son. "Axborotlashtirish to'g'risida".
3. O'zbekiston Respublikasining Qonuni, 29.09.2022 yildagi O'RQ-792-son. "Elektron tijorat to'g'risida".
4. United Nations. Guidelines for Action to Combat Cyber Violence Against Women. New York: United Nations. 2020.
5. Ministry of Internal Affairs of the Republic of Uzbekistan. 2024 Annual Cybercrime Report — Statistical insights on cybercrime rise and patterns in Uzbekistan.
6. O'zbekiston Respublikasi Jinoyat kodeksi. <https://lex.uz/docs/-111453>