

Gender Equality in Cyberspace and Cyber Violence Against Women

 Uktamova Sevinch Uktam qizi

Tashkent State University of Law, Tashkent, Uzbekistan

Received: 23 August 2026; **Accepted:** 19 September 2026; **Published:** 13 October 2026

Abstract: Today, the rapid development of digital technologies is influencing all spheres of society. In this context, cyberspace has become not only a means of information exchange but also an important environment where social relations are formed. At the same time, new types of problems are spreading widely in this environment, particularly cases of cyber violence against women. In particular, gender equality is one of the fundamental principles of modern society and implies equal rights and opportunities for men and women. However, this equality is often violated in the online world. Specifically, women on social networks and other online platforms are more frequently subjected to insults, threats, and pressure. This negatively affects their ability to freely express their opinions and to actively participate in social life.

Keywords: Cyber violence, young girls and women, online threats, cyberstalking, trolling, doxing, non-consensual images, gender equality.

Introduction: In recent years, the expansion of the internet, widespread use of mobile technologies, and social networking have given rise to the issue of gender equality in cyberspace, including new forms of violence against women and girls (VAWG), specifically cyber VAWG. The COVID-19 pandemic further accelerated this trend by shifting women's employment, education, and social activities online. Cyber VAWG negatively impacts not only the health and well-being of women but also economic, social, and political spheres. Because online and offline violence are frequently interrelated, existing legislative frameworks are failing to keep pace with technological advancements. Therefore, it is imperative that the digital space becomes a safe environment for women and girls. According to Article 48 of the Constitution of the Republic of Uzbekistan, women and girls, and men have equal rights [1]. This constitutional norm is directly linked to ensuring that women and men possess equal rights and freedoms in both online and real-world settings.

Consequently, the relevance of this research lies in addressing the current legislative gap where gender

disparities occurring in the physical realm are being mirrored in cyberspace, thereby necessitating clear and adequate legal regulation of liability.

METHODS

During the analysis process, the following forms of cyber VAWG are examined, including sexual harassment, stalking, zoombombing [2], non-consensual sharing of intimate images, trolling [3], doxing [4], misogynistic or gender-based hate speeches, as well as digital-facilitated manifestations of intimate partner or domestic violence. Furthermore, the analysis of this study comprises four stages. In the first stage, the current legislation of the Republic of Uzbekistan is analyzed. Specifically, mechanisms for protecting personal data in the online environment are examined based on the Criminal Code of the Republic of Uzbekistan [5], as well as the Laws "On Informatization" [6], "On Personal Data" [7], and "On Cybersecurity" [8]. In the second stage, international legislative sources and foreign legal experiences related to this subject are studied. In particular, the UN Convention on the Elimination of All Forms of Discrimination Against Women [9], the Council of

Europe Convention on Cybercrime (Budapest Convention, 2001) [10], and the European Union's digital safety approaches are investigated to analyze mechanisms for detecting and preventing offenses in cyberspace. In the third stage, a qualitative analysis is conducted based on academic papers and scholarly research. Additionally, an analysis grounded in international experience is performed. In the fourth stage, international statistical indicators concerning gender equality in cyberspace and cyber violence against women are analyzed.

RESULTS AND DISCUSSION

Today, cyber violence against women and girls (CVAWG) is emerging as a widespread and systemic problem in the modern digital space. According to analyses, women suffer more frequently and severe forms of harm from online violence compared to men. In particular, they are more likely to encounter continuous psychological pressure, threats, insults, and violations of privacy. The specific characteristics of cyber violence, including anonymity, rapid dissemination, and the long-term persistence of harmful content, significantly amplify its impact. These factors further complicate the issue for victims, making it difficult to control the scope of violence and to halt it. Specifically, the findings highlight online harassment, cyberstalking, non-consensual dissemination of personal or intimate content, threats, abusive messages, and other related acts as the most prevalent forms of cyber violence.

Specifically, ensuring cybersecurity in the Republic of Uzbekistan is implemented through strict adherence to the Constitution of the Republic of Uzbekistan, current laws, and other regulatory legal acts. Any violation of legal requirements entails liability in any form. In particular, the Law of the Republic of Uzbekistan "On Cybersecurity" constitutes an important legal framework in combating online violence and cyberattacks. According to Article 6 of this Law, protecting the interests of the individual, society, and the state in cyberspace is of paramount importance, serving as a core principle in the state's cybersecurity policy [8]. Furthermore, a unified approach in the field of cybersecurity ensures effective management of the national cyber defense system through data protection, implementation of software and technical tools, monitoring of information systems, and organization of oversight. Additionally, violence against women in cyberspace – and violence in general – constitutes an infringement upon personal data. The Law of the Republic of Uzbekistan "On Personal Data" applies to the collection, storage, systematization, modification, dissemination, and destruction of personal data; however, it does not apply to

operational-search activities, intelligence, crime suppression, or information related to state secrets [7]. The Law is formulated based on the principles of respecting constitutional human and civil rights, utilizing data for lawful purposes, ensuring accuracy and confidentiality, and providing equal protection for the rights of subjects, owners, and operators.

As noted above, findings demonstrate that cyberstalking and cyberbullying are widely prevalent as major forms of cyber violence. Cyberstalking typically exhibits a systematic and repetitive nature, undermining the victim's sense of safety. It frequently manifests through sending threatening messages, online insults, and non-consensual sharing of personal or intimate materials. Modern technologies (GPS, geolocation services, social networks) further exacerbate cyberstalking, enabling continuous surveillance of the victim. This phenomenon is particularly prevalent within the context of intimate partner violence. Online hate speech targeted at women is usually associated with sexual objectification, body-shaming, offensive comments, and rape threats, often perpetrated by members of incel communities. On online platforms, hate speech is difficult to monitor and counteract due to anonymity, rapid dissemination, and simultaneous execution by multiple aggressors.

Non-consensual intimate image abuse refers to the distribution of a person's sexual or intimate materials through social networks or websites without their consent [11]. In these cases, victims are predominantly women, and the acts are often committed by former partners. This category includes digital voyeurism – namely "upskirting" and "downblousing" – as well as cyber flashing and deepfake content. In this process, intimate materials are frequently used for sextortion (sexual extortion), where money, other materials, or sexual favors are demanded under the threat of disseminating sexual or intimate images. Under Article 141-3 of the Criminal Code of the Republic of Uzbekistan, disseminating information containing nude photographic and/or video images of a person's body or genitalia without their consent, including dissemination in mass media, telecommunication networks, or the global Internet, or threatening to disseminate such information, is punishable by a fine from four hundred to six hundred times the base calculation amount, or mandatory community service up to three hundred sixty hours, or correctional labor up to three years [12].

Trolling and gender-trolling exert psychological pressure by drawing individuals into unnecessary and unproductive disputes within online discussions. Trolling is typically conducted anonymously and encompasses insults, sexual threats, and rape threats

directed at women. Article 140 of the Criminal Code of the Republic of Uzbekistan regulates “insult”, which is also applied to online insults. According to this article, insult – that is, the intentional degradation of an individual’s honor and dignity in an indecent manner, if committed after the application of an administrative penalty for such actions – is punishable by a fine up to two hundred times the base calculation amount, or mandatory community service up to two hundred forty hours, or correctional labor up to one year [12].

It can be asserted that such actions are employed to manipulate online communities, exclude new users, and restrict constructive discussions. Furthermore, doxing (disclosure of personal data) involves the collection and public dissemination of a victim’s personal and sensitive information without consent. This information encompasses residential addresses, photographs, and family details. Doxing heightens psychological stress and exposes the victim to physical harm. It is frequently utilized in conjunction with other forms of cyber violence, rendering it particularly dangerous in the context of gender-based violence. Analyzing this issue under Uzbek legislation, Article 141-1 of the Criminal Code provides that unlawful collection or dissemination of information concerning a person’s private life constituting personal or family secrets, committed without consent after administrative penalties have been applied for similar acts, shall be punished by a fine from fifty to one hundred times the base calculation amount, or mandatory community service up to three hundred hours, or correctional labor up to two years [12].

According to studies, cyber violence – including acts such as sending repetitive messages and doxing – ranks among the most widespread forms of cyber violence globally. Regional and cross-country studies further confirm the urgency of this issue. For instance, a multi-country survey conducted in 2017 involving women aged 18-55 across Denmark, Italy, New Zealand, Poland, Spain, Sweden, the UK, and the USA revealed that nearly a quarter of women (23%) had experienced online abuse [13]. Although men can also experience online violence, women and girls are significantly more exposed to gender-specific forms of violence in digital environments. For example, in the USA, 33% of women under 35 reported experiencing online sexual harassment, whereas only 11% of men reported similar experiences. Furthermore, 47% of women reported experiencing online harassment due to their gender, compared to only 18% of men (GREVIO, 2021) [14]. A study conducted in India revealed that 31% of women had encountered online sexual harassment and that online VAWG (Violence Against Women and Girls) can migrate from one platform to another; for instance,

men rejected on dating platforms were observed sending repeated friend requests to women on platforms like Facebook [14].

Online violence and cyber threats against women vary among different groups. Young girls and women are particularly vulnerable, as their online engagement, information consumption, and peer interactions expose them to higher levels of threats. According to global studies, 58% of girls and a significant proportion of young women have encountered online harassment [15]. Women with disabilities, LGBTIQ individuals, or members of minority groups also face heightened vulnerability to cyber violence. For example, US studies indicate that lesbian, gay, or bisexual individuals experience higher levels of online abuse due to the intersection of gender and sexual orientation [16]. Similarly, women with intellectual or cognitive disabilities can be targeted through technology. Moreover, women engaged in public life – including human rights activists, politicians, and journalists – are at the highest risk. Up to 73% of female journalists have encountered online abuse, including physical and sexual threats, as well as attacks on their digital security [17]. Among female parliamentarians in Africa, 46% have been targeted by online sexist attacks. Politically active women face insults, hate speech, defamation, and physical as well as sexual threats [18].

This matter is comprehensively and explicitly regulated in international legal instruments. Specifically, Article 1 of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) clarifies the concept of “discrimination against women”, defining it as any distinction, exclusion, or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment, or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil, or any other field [9]. Furthermore, under Article 2 of the Convention, States Parties are obligated to pursue by all appropriate means a policy of eliminating discrimination against women, taking necessary legal and institutional measures. The goal of adopting all appropriate measures by States Parties is to modify the social and cultural patterns of conduct of men and women, with a view to achieving the elimination of prejudices and customary and all other practices which are based on the idea of the inferiority or the superiority of either of the sexes or on stereotyped roles for men and women [9].

It can be concluded that today, cyber violence must be interpreted not merely as a simple social issue, but as a systemic violation of human rights and freedoms. In

particular, online threats and various forms of digital coercion targeting women represent a reflection of existing gender inequality in cyberspace, closely tied to deeply rooted societal stereotypes and discriminatory attitudes. Therefore, developing a zero-tolerance approach toward cyber violence holds substantial scientific and practical significance.

CONCLUSION

The above analysis indicates that cyber violence against women and girls today constitutes a widespread and complex socio-legal issue within the modern digital environment. Its manifestations, such as cyberstalking, trolling, doxing, and the non-consensual dissemination of intimate materials, cause severe harm not only to an individual's honor and dignity but also to their physical safety and psychological well-being. Furthermore, characteristics of cyber violence such as anonymity, rapid dissemination, and complexity of control further exacerbate this challenge. Although the Republic of Uzbekistan possesses a legal framework aimed at ensuring cybersecurity and personal data protection – including the Law of the Republic of Uzbekistan “On Cybersecurity” [8] and the Law of the Republic of Uzbekistan “On Personal Data” [7], among others – the current legislative framework does not comprehensively address cyber violence against women as a distinct legal offense. Instead, such acts are currently evaluated under general provisions of the Criminal Code of the Republic of Uzbekistan, such as provisions governing insult, violation of privacy, or unlawful dissemination of information. This prevents full consideration of the unique characteristics of cyber violence and creates specific operational difficulties in law enforcement practice. Consequently, the lack of explicit and specialized statutory provisions in the legislation indicates a noticeable legal gap.

Therefore, it is advisable to put forward the following recommendations: First, it is necessary to recognize cyber violence against women as a distinct legal institution and incorporate specialized norms into national legislation that clearly define its primary forms (cyberstalking, cyberbullying, doxing, non-consensual distribution of intimate materials, etc.). Second, liability for cyber violence should be strengthened, specifically establishing aggravating circumstances when victims are women or minors. Third, to enhance law enforcement practice, judicial and law enforcement personnel should undergo continuous and systematic professional training regarding digital crimes and cyber violence.

REFERENCES

1. Constitution of the Republic of Uzbekistan (2023). Article 48. LexUZ Legal Database.
2. Sexual Violence Research Initiative. (2020). Online safety in a changing world – COVID-19 and cyber violence.
3. United Nations Human Rights Council. (2018). Report on online violence against women and girls (A/HRC/38/47, para. 23).
4. United Nations Human Rights Council. (2020). Report on freedom of opinion and expression in the digital age (A/HRC/44/52).
5. Criminal Code of the Republic of Uzbekistan (1994, as amended). LexUZ Legal Database. <https://lex.uz/mact/-111453>
6. Law of the Republic of Uzbekistan. (2003). On Informatization (No. 560-II). LexUZ Legal Database. <https://lex.uz/docs/-6445145>
7. Law of the Republic of Uzbekistan. (2019). On Personal Data (No. ZRU-547). LexUZ Legal Database. <https://lex.uz/docs/-6445145>
8. Law of the Republic of Uzbekistan. (2022). On Cybersecurity (No. ZRU-764). LexUZ Legal Database. <https://lex.uz/uz/docs/-5960604>
9. United Nations General Assembly. (1979). Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). LexUZ Legal Database. <https://lex.uz/docs/-2685528>
10. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). UzPedia. https://uzpedia.uz/pedia/kiberjinoatlar_togrisida_konvensiya
11. UN Women. (2021). Violence against women in the online space: Insights from a multi-country study in the Arab States.
12. Criminal Code of the Republic of Uzbekistan (1994, as amended). LexUZ Legal Database. <https://lex.uz/mact/-111453>
13. Amnesty International. (2017, November 20). Amnesty reveals alarming impact of online abuse against women. <https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/>
14. Gurumurthy, A., Vasudevan, A., & Chami, N. (2019). Born digital, born free? A socio-legal study on young women's experiences of online violence in South India. IT for Change. https://itforchange.net/sites/default/files/1662/Born-Digital_Born-Free_SynthesisReport.pdf
15. Plan International. (2020). Free to be online? Girls' and young women's experiences of online

harassment.

- 16.** Pew Research Center. (2021). The state of online harassment.
- 17.** UNESCO. (2020). Online violence against women journalists: A global snapshot of incidence and impacts.
- 18.** Inter-Parliamentary Union. (2021). Sexism, harassment and violence against women in parliaments in Africa.