PROTECTION OF WOMEN IN THE REPUBLIC OF UZBEKISTAN FROM HARASSMENT AND VIOLENCE COMMITTED IN CYBERSPACE: A COMPARATIVE ANALYSIS AND PROPOSALS

Khudoyberganova Feruza Bahodir qizi
Juvenile Inspector-Psychologist, Department of Internal Affairs

Abstract: The article provides a systematic analysis of the current legislation of the Republic of Uzbekistan in the field of protecting women from harassment and violence committed in cyberspace and identifies the existing legal gaps. By comparing the national regulatory framework with international standards, the author substantiates nine conceptual gaps: the absence of a definition of cyber violence, the lack of liability for the non-consensual dissemination of intimate images, the absence of legal regulation of deepfakes, the failure of the protection order to cover the digital dimension, the indeterminacy of the content removal period, and the non-disaggregation of the online modality in statistical reporting.

Based on the research findings, de lege ferenda proposals have been developed: a draft of specific provisions to be introduced into the Law on Protection of Women from Harassment and Violence, the Criminal Code, the Code of Administrative Liability and the Law on Informatization is proposed. The concept of a phased implementation of the reform and a system of indicators for assessing its effectiveness are substantiated.

Keywords: cyber violence, legislative improvement, protection order, non-consensual intimate images, deepfake, doxing, criminal liability, information intermediary, legal gap, de lege ferenda.

Significant legal reforms have been implemented in the Republic of Uzbekistan in recent years in the field of protecting the rights of women. The Law of the Republic of Uzbekistan "On Protection of Women from Harassment and Violence," adopted on 2 September 2019, became the country's first special law in this field and introduced the institution of the protection order. By Law No. O'RQ-829 of 11 April 2023, Article 126-1 ("Domestic Violence") was introduced into the Criminal Code, strengthening liability for violence. Article 34 of the Constitution in its 2023 edition enshrines everyone's right to privacy, while Article 58 establishes the State's obligation to protect the family.

At the same time, these reforms have been directed almost entirely at the offline environment—within the family, mahalla, and workplace—while violence committed in the digital environment has in practice remained outside the focus of legislation. The 2022 assessment of the United Nations Development Programme directly noted that "no policies on gender-based online violence, cyberbullying or online violence were identified" in Uzbekistan. This situation is inconsistent with the objectives of digital transformation and human rights protection established in the "Development Strategy of New Uzbekistan for 2022–2026," because, amid the rapidly increasing level of internet use among the population,

the failure to extend legal protection to the digital environment creates a zone of vulnerability for women.

The purpose of this article is to critically analyse the current national legislation through the prism of international standards and foreign experience, systematise the identified legal gaps, and develop specific, normatively formulated proposals for legislative reform.

In the legislation of the Republic of Uzbekistan, provisions relevant to cyber violence are dispersed across five groups of legal instruments.

The first group comprises the special law. Article 3 of the Law "On Protection of Women from Harassment and Violence" defines four types of violence: physical, psychological, sexual and economic. The only direct reference to the digital environment remains within the definition of "harassment": "pursuing a person, monitoring them, or attempting to establish contact with them through telecommunication networks, including the Internet." Although this formulation was progressive for its time, it is purely definitional in nature and is not supported by an independent sanctioning provision. Article 23-1, introduced in the 2023 edition of the Law, reduced the period for issuing a protection order to 24 hours, established its validity period as 30 days, and provided for its extension by a court for up to one year.

The second group comprises criminal-law provisions. A number of articles of the Criminal Code identify commission through the Internet as an aggravating circumstance: Article 103 (incitement to suicide), Article 103-1 (coercion to suicide), Article 130 (distribution of pornographic materials), Article 139 (defamation), and Article 140 (insult). Article 141-1 establishes liability for the unlawful collection, dissemination or disclosure of information relating to private life (it should be noted that Article 141 concerns violations of the equality of citizens, as these provisions are often confused in the literature). Article 126-1 provides for liability for domestic violence.

The third group comprises administrative-law provisions. Article 41-1 of the Code of Administrative Liability establishes liability for sexual harassment, Article 59-2 for domestic violence, and Article 206-1 for violation of the requirements of a protection order; Part 2 of Article 46-2 provides for liability for the unlawful processing of personal data using artificial intelligence technologies. Although the latter provision is the rule most closely related to the deepfake problem, it is based on the logic of data protection and does not reflect the social danger of creating sexually explicit synthetic content.

The fourth group comprises provisions in the information sphere. Article 12-1 of the Law "On Informatization" imposes on website owners and hosting providers an obligation to remove prohibited information "immediately." This creates a serious problem for law enforcement practice: the concept of "immediately" is an evaluative category not limited by a specific period, which in practice makes it difficult to monitor compliance with the obligation and impose liability for its violation. The fifth group is the Law "On Personal Data," which establishes the rights of data subjects but does not provide special expedited mechanisms for cases involving violence.

From a doctrinal perspective, these issues have been partially addressed by Kh.Kh. Saydivaliyeva and U.Sh. Khamrakulov, K. Alieva, A.R. Kurmychkina, and K.Z. Sharipova and R.M. Turimbetov. The authors unanimously note that cyber violence has not yet developed as an independent legal category in national legislation. Sh.A. Normatova substantiates the need to expand the doctrinal boundaries of the concept of violence, while S.K. Alimov emphasises the comprehensive nature of the protection system; Sh.A. Pulatova and A.Sh. Murodov have developed practical methods for working with victims. M.R. Almamatova stresses the interrelationship of social and legal measures in preventing violence.

Law-enforcement statistics demonstrate that the protection system is actively functioning. While 32,733 protection orders were issued in 2023, this figure reached 55,757 in the first half of 2025. During 2024, 472 persons were convicted under Article 126-1 of the Criminal Code; 16,524 cases were considered under Article 59-2 of the Code of Administrative Liability, and 1,854 cases under Article 41-1.

However, none of these data are disaggregated according to the modality of violence—namely, whether it was committed in an offline or online environment. Cyber violence is likewise not maintained as a separate indicator in the Statistics Agency's gender statistics database. From a methodological perspective, this creates a twofold problem: first, it becomes impossible to assess the actual scale of the problem; second, the empirical basis for developing evidence-based policy is lost. For precisely this reason, paragraph 34(b) of the CEDAW Committee's General Recommendation No. 35 requires States to collect data covering technology-facilitated violence.

A gap is also observed at the level of international monitoring mechanisms. The 2022 concluding observations of the CEDAW Committee concerning Uzbekistan's sixth periodic report did not address online or digital violence at all; the document contains no relevant recommendations. This may be characterised as a dual gap: the problem is not covered not only in national legislation but also at the international monitoring level. The Ombudsman's 2025 methodological guide likewise recognises that cyberbullying has not been established as a separate criminal offence and may be qualified only under existing general offences.

In the regional context, a 2023 study by UN Women estimates the prevalence of technology-facilitated violence in Central Asia at 38.6%, while only 43.8% of victims reported it to someone. Although Uzbekistan was not included in the study sample, based on data from neighbouring countries with similar socio-cultural conditions, it is reasonable to conclude that the problem also exists on a significant scale in the country.

A comparison of the current legislation with the minimum standards established by Directive (EU) 2024/1385, GREVIO General Recommendation No. 1, and Article 16 of the United Nations Convention against Cybercrime makes it possible to identify nine systemic gaps.

1. The concept of cyber violence (digital violence) is not defined in legislation at all. The existing four-category classification does not take into account the environment in which violence is committed.

2. No specific liability is established for the non-consensual dissemination of intimate images (NCII). Article 130 penalises the distribution of pornography; however, its protected interest is public morality rather than the victim's sexual autonomy. Moreover, there is a risk that the victim herself may be held liable under this provision, which constitutes a serious barrier to reporting.

3. Sexually explicit synthetic materials created using artificial intelligence (deepfakes) are not legally regulated. Part 2 of Article 46-2 of the Code of Administrative Liability covers only the data-processing aspect.

4. Cyberstalking has not been established as an independent criminal offence; the definition of "harassment" is not linked to a sanction.

5. No liability is provided for sexual extortion (sextortion) or gender-based doxing.

6. The content of the protection order does not cover the digital dimension: it does not establish a prohibition on digital communication, publication of the victim's images, communication through third parties, or the use of spyware.

7. The period for removing content is not clearly defined—the evaluative category "immediately" is used, and there is no direct reporting procedure for victims.

8. There are no specific obligations for information intermediaries to prevent gender-based violence, nor is there an institution of a competent authority to supervise such obligations.

9. Online modality is not distinguished in statistical reporting, resulting in an ineffective monitoring and evaluation system.

Analysis of these gaps demonstrates that they are not accidental but stem from a single systemic cause: legislation understands violence primarily as an event occurring in physical space. Therefore, rather than addressing the gaps separately, a comprehensive conceptual reform is required.

In order to eliminate the identified gaps, we propose introducing the following regulatory amendments.

The first direction is improvement of the special law. It is proposed to supplement Article 3 of the Law "On Protection of Women from Harassment and Violence" with the following definition: "digital (cyber) violence means any act partially or wholly committed, facilitated or aggravated through information and communication technologies, directed against a woman because of her sex and causing, or creating a risk of causing, physical, psychological, sexual or economic harm to her." This formulation fully corresponds to the definition contained in the report of the UN Special Rapporteur A/HRC/38/47 and ensures harmonisation of national legislation with international standards. In accordance with the classification in GREVIO General Recommendation No. 1, at least five forms of digital violence—non-consensual dissemination of intimate images, cyberstalking, sexual extortion, doxing, and coordinated (group-based) harassment—should also be expressly listed in the text of the law.

The provisions of the Law concerning protection orders should be supplemented with digital prohibitions. In this regard, the experience of the Kyrgyz Republic—defining "communication" so as to include communication through messengers, email and social networks—may be directly incorporated. It is proposed that the protection order include: a prohibition on communication through any digital channel; a prohibition on publishing information and images concerning the victim; a prohibition on contacting the victim through third parties or anonymous accounts; and a prohibition on the use of geolocation and surveillance software.

The second direction is criminal-law regulation. It is proposed to introduce a new article into the Criminal Code entitled "Non-Consensual Dissemination of Intimate Images." Its disposition could be formulated as follows: "Dissemination, publication or otherwise making available an intimate image of a person without that person's consent by means of information and communication technologies." The second part of the article should also establish liability for materials created using artificial intelligence or other technical means that depict a person as participating in sexually explicit acts. This would be consistent with Article 5(1)(b) of the EU Directive, the concept of "digital forgery" under the U.S. TAKE IT DOWN Act, and Article 14-2 of the legislation of the Republic of Korea. The third part should provide liability for threats to disseminate an image (following the structure of section 66B(4) under the UK model) and for sexual extortion. As an important legal safeguard, an explanatory note should expressly establish that consent to creating an image or sending it to a particular person does not constitute consent to its dissemination to third parties.

In addition, it is recommended to establish "Cyberstalking" as an independent offence. Following the model of Section 238 of the German Criminal Code, its disposition should include repeated attempts to contact a person through telecommunications, misuse of personal data, publication of false content in the victim's name, and dissemination of the victim's images. Particular attention should be paid to coordinated harassment: drawing on the experience of the "en meute" construction in Article 222-33-2-2 of the French Criminal Code, a provision should be introduced allowing each participant in group-based harassment to be held liable even where the individual participant does not, on their own, satisfy the element of repetition.

The third direction is administrative liability. It is proposed to introduce into the Code of Administrative Liability a provision establishing liability for acts that are not sufficiently socially dangerous to warrant criminal liability—online insult, discrimination, gender-based harassment, and less serious forms of doxing. The experience of Article 127-2 of the Code of Administrative Offences of the Republic of Kazakhstan may be useful, but its limitation to the protection of minors should not be replicated; the provision should apply to all persons, while commission on the basis of gender should constitute an aggravating circumstance.

The fourth direction is information-sector obligations and an institutional mechanism. It is proposed to replace the evaluative term "immediately" in Article 12-1 of the Law "On Informatization" with a specific period for materials related to violence. In international

practice, this period is set at 24 hours: sections 77–80 of Australia's 2021 legislation and Rule 3(2)(b) of India's 2021 Rules provide for such a period. At the same time, a direct notice-and-takedown procedure for victims should be established at the legislative level, and the material should be temporarily blocked while the complaint is being reviewed.

Institutionally, Australia's eSafety Commissioner model is assessed as the most effective solution. Its statistical results—more than 98% of 7,270 reports resolved in 2023–2024, with only four formal enforcement notices issued—demonstrate that the system operates primarily on a cooperative basis. In Uzbekistan, it would be appropriate to introduce such powers as a specialised unit within an existing competent state authority rather than establish a new body, thereby minimising budgetary expenditure. In regulating platform responsibility, Article 34(1)(d) of the EU Digital Services Act—recognising gender-based violence as a systemic risk—may serve as a conceptual guide.

The fifth direction is procedural and statistical support. The procedure for collecting electronic evidence and ensuring its prompt preservation should be improved; the mechanisms developed under the Budapest Convention and the international cooperation institutions provided for by the United Nations Convention against Cybercrime may serve as a basis. In legal statistics, separate recording of violence cases by online modality should be introduced, and the indicator system developed by EIGE and the OHCHR 2025 methodological tool should be adopted as a basis for assessment.

Given the scope of the proposed changes, it would be appropriate to implement the reform in three stages. At the first stage (short term), the definition of cyber violence should be introduced into the special law, the protection order should be supplemented with digital prohibitions, and statistical reporting should be improved; these measures do not require significant budgetary expenditure and can produce rapid results. At the second stage (medium term), amendments should be made to the Criminal Code and the Code of Administrative Liability, and specialised training programmes should be introduced for law-enforcement personnel. At the third stage (long term), an institutional mechanism for cooperation with information intermediaries should be established and integration into the international cooperation system ensured.

The following indicators are recommended for assessing the effectiveness of the reform: the number of protection orders containing digital prohibitions; the ratio of criminal cases initiated for cyber violence to court judgments rendered in such cases; the number of requests for content removal and the average processing time; and the rate at which victims report incidents (based on periodic sociological surveys to assess underreporting). These indicators are consistent with the EIGE methodology and also enable international comparative analysis.

It should be emphasised that improving legislation alone is not sufficient. The obligations set out in Articles 33, 34 and 40 of the Istanbul Convention require States to take not only regulatory but also organisational, educational and preventive measures. As Sh.A. Pulatova and A.Sh. Murodov emphasise, legal assistance to victims must be closely integrated with psychological and social rehabilitation; S.K. Alimov, based on an analysis of foreign

experience, substantiates that the effectiveness of a protection system depends on its comprehensive and multi-stage structure.

The following conclusions were reached on the basis of the research conducted.

First, although the system for protecting women from violence in the legislation of the Republic of Uzbekistan has developed significantly, it is conceptually oriented towards the offline environment. Cyber violence has not developed as an independent legal category, and the only relevant provision—the digital reference contained in the definition of "harassment"—remains a declarative rule not linked to a sanction.

Second, the analysis identified nine systemic legal gaps, the most serious of which are the absence of liability for the non-consensual dissemination of intimate images and the creation of synthetic sexual content (deepfakes). Attempts to qualify such acts under the existing Articles 130 or 141-1 are legally imperfect and do not adequately protect victims' interests.

Third, the failure to distinguish online modality in statistical reporting precludes assessment of the actual scale of the problem and the development of evidence-based legal policy. This gap was also not addressed in the CEDAW Committee's 2022 concluding observations, meaning that it has remained overlooked at the international monitoring level as well.

Fourth, an analysis of foreign experience shows that an effective protection system consists of four elements: a clear legal definition of cyber violence, independent criminal offences, a content-removal mechanism with a specified time limit, and a competent authority responsible for its supervision. Each of these four elements can be introduced in Uzbekistan, but this requires adaptation that takes into account the specific features of the national legal system rather than mechanical transplantation of foreign models.

Fifth, the legal basis for the proposed reform is strong: it is fully consistent with the right to privacy enshrined in Article 34 of the Constitution, the country's international obligations under the CEDAW Convention, and the digital transformation objectives established in the Development Strategy. The phased implementation of the reform will ensure its financial and institutional feasibility.

REFERENCES

1. Constitution of the Republic of Uzbekistan (2023 edition). // https://lex.uz/docs/-6445145

2. Law of the Republic of Uzbekistan No. O'RQ-561 of 2 September 2019 "On Protection of Women from Harassment and Violence." // https://lex.uz/docs/-4494709

3. Law of the Republic of Uzbekistan No. O'RQ-829 of 11 April 2023. // https://lex.uz/ru/docs/-6430272?ONDATE=12.04.2023%2000

4. Criminal Code of the Republic of Uzbekistan. // https://lex.uz/docs/-111453

5. Code of the Republic of Uzbekistan on Administrative Liability. // https://lex.uz/docs/-97664

6. Law of the Republic of Uzbekistan "On Informatization," Article 12-1. // https://lex.uz/docs/-83472

7. Law of the Republic of Uzbekistan "On Personal Data." // https://lex.uz/docs/-4396428

8. Decree of the President of the Republic of Uzbekistan No. PF-60 of 28 January 2022. // https://lex.uz/docs/-5841063

9. CEDAW Committee. General recommendation No. 35 (2017), CEDAW/C/GC/35. // https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-35-2017-gender-based

10. CEDAW Committee. Concluding observations on the sixth periodic report of Uzbekistan, CEDAW/C/UZB/CO/6 (2022). // https://www.ohchr.org/en/documents/concluding-observations/cedawcuzbco6-concluding-observations-sixth-periodic-report

11. Report of the Special Rapporteur on violence against women, A/HRC/38/47 (2018). // https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and

12. GREVIO General Recommendation No. 1, GREVIO(2021)20. // https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

13. Council of Europe Convention CETS No. 210 (Istanbul Convention). // https://rm.coe.int/168008482e

14. Convention on Cybercrime (ETS No. 185), Budapest, 2001. // https://rm.coe.int/1680081561

15. United Nations Convention against Cybercrime, A/RES/79/243 (2024). // https://treaties.un.org/doc/Publication/CTC/Ch_XVIII_16.pdf

16. Directive (EU) 2024/1385 of 14 May 2024. // https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng

17. Regulation (EU) 2022/2065 (Digital Services Act). // https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

18. Online Safety Act 2023 (UK), ss. 187–188. // https://www.legislation.gov.uk/ukpga/2023/50/section/188

19. Online Safety Act 2021 (Australia). // https://www.legislation.gov.au/C2021A00076/latest/text

20. ACMA – eSafety Commissioner. Annual Report 2023–24. // https://www.esafety.gov.au/sites/default/files/2024-10/ACMA-eSafety-annual-report-2023-24.pdf

21. TAKE IT DOWN Act, Public Law 119–12 (2025). // https://www.congress.gov/119/plaws/publ12/PLAW-119publ12.pdf

22. Act on Special Cases concerning the Punishment of Sexual Crimes (Republic of Korea). // https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=68812&key=&type=new

23. Criminal Code of Germany (Strafgesetzbuch), § 238. // https://www.gesetze-im-internet.de/stgb/__238.html

24. French Criminal Code (Code pénal), Article 222-33-2-2. // https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049312743

25. Italian Criminal Code (Codice penale), Article 612-ter. // https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.idArticolo=10&art.codiceRedazionale=19G00076

26. Information Technology (Intermediary Guidelines) Rules 2021 (India). // https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

27. Code of the Republic of Kazakhstan on Administrative Offences, Article 127-2. // https://prg.kz/document/print/?doc_id=37059864

28. Law of the Kyrgyz Republic No. 63 of 27 April 2017. // https://cbd.minjust.gov.kg/4-2381/edition/14086/ru

29. UN Women ECA. The dark side of digitalization. — 2023. // https://eca.unwomen.org/sites/default/files/2024-01/research-tf-vaw_full-report_24-january2.pdf

30. UNDP. Gender Digital Divide Assessment: Uzbekistan. — 2022. // https://www.undp.org/sites/g/files/zskgke326/files/2023-03/Final_Gender%20Digital%20Divide%20in%20Uzbekistan_d.pdf

31. OHCHR. Tool on technology-facilitated gender-based violence. — 2025. // https://www.ohchr.org/sites/default/files/documents/issues/women/genderandequality/2025-tool-technology-facilitated-gbv.pdf

32. EIGE. Cyber violence against women. // https://eige.europa.eu/gender-based-violence/cyber-violence-against-women

33. Ombudsman. Guide on Gender-Sensitive Legal Assistance. — Tashkent, 2025. // https://ombudsman.uz/uploads/2025/11/genderganisbatansezgiryuridikyordam0-3.pdf

34. Gazeta.uz. Statistics on protection orders. — 11 July 2025. // https://www.gazeta.uz/oz/2025/07/11/himoya-orderi/

35. Kun.uz. Judicial practice statistics on domestic violence. — 14 October 2025. // https://kun.uz/news/2025/10/14/ozbekistonda-81-kishi-oilaviy-zoravonlik-uchun-ozodlikdan-mahrum-etildi

36. Statistics Agency of the Republic of Uzbekistan. Gender Statistics. // https://gender.stat.uz/uz/

37. Pulatova Sh.A., Murodov A.Sh. Protection of the Rights of Victims of Violence and Prevention of Violence. — Tashkent: Baktria Press, 2020. — 56 p.

38. Alimov S.K. A Comprehensive Systemic Approach to Preventing Violence against Women: International Experience // Academic Research in Educational Sciences. — 2023. — Vol. 4, Issue 1. — pp. 436–446.

39. Normatova Sh.A. The Concept of Harassment and Violence against Women and Its Specific Features. — pp. 103–110.

40. Almamatova M.R. Social and Legal Foundations for Preventing Violence against Women and Girls in Uzbekistan. — pp. 292–294.

41. Saydivaliyeva Kh.Kh., Khamrakulov U.Sh. Cyber Violence as a Form of Violence against Women and Its Types. — Tashkent, 2023. // https://cdn.uza.uz/2023/07/28/10/27/ACpVa6SAGsKAs8DjJ13qzas8RaPB0IiE.pdf

42. Alieva K. Online Gender-Based Violence in Uzbekistan: Gaps in Legislation and the Path Forward. — 2025. // https://ilmiykutubxona.uz/id/eprint/405

43. Kurmychkina A.R. Digital Violence and Harassment against Women. // https://inlibrary.uz/index.php/zdift/article/view/79517

44. Sharipova K.Z., Turimbetov R.M. Legal Protection of Women of the Republic of Uzbekistan from Digital Violence. // https://lajoe.org/index.php/LAJoE/article/view/1108