CYBERVIOLENCE AND LEGAL PROTECTION: LESSONS FROM UZBEKISTAN AND THE EUROPEAN UNION

Khamraeva Shakhnoza, Social specialist at
International Consulting Company "Juru"
E-mail: hamroyeva@gmail.com

Annotation. This article accentuates on cyberviolence as a growing threat to women and children, analyzing Uzbekistan's current legal framework and comparing it with the European approaches to protecting individuals from online abuse, including the United Kingdom's Online Safety Bill (2023) and the European Union's Digital Services Act (2024). The study identifies gaps in national legislation, highlights international best practices, and proposes recommendations for strengthening protection in Uzbekistan's digital space.

Key words: cyberviolence, women, children, Online Safety Bill, Digital Services Act.

KIBERZO'RAVONLIK VA HUQUQIY HIMOYA: O'ZBEKISTON VA YEVROP ITTIFOQI TAJRIBASI

Hamrayeva Shahnoza Atadjanovna,
"Juru" xalqaro konsalting firmasida,
Ijtimoiy masalalar bo'yicha mutaxassis
E-mail: hamroyeva@gmail.com

Annotatsiya. Ushbu maqolada kiberzo'ravonlik ayollar va bolalar uchun ortib borayotgan tahdid sifatida ko'rib chiqilgan bo'lib, unda O'zbekistonning bu sohadagi amaldagi huquqiy bazasi tahlil qilinadi va onlayn zo'ravonlikdan himoya qilish bo'yicha Yevropa yondashuvlari, jumladan, Buyuk Britaniyaning «Onlayn xavfsizlik to'g'risida»gi qonuni (2023-y.) va Yevropa Ittifoqining «Raqamli xizmatlar to'g'risida»gi reglamenti (2024-y.) bilan taqqoslanadi. Tadqiqotda milliy qonunchilikdagi bo'shliqlar ko'rsatiladi, xalqaro ilg'or tajribalar yoritiladi va O'zbekistonning bu boradagi qonunchiligini mukammallashtirish bo'yicha takliflar beriladi.

Kalit so'zlar: kiberzo'ravonlik, ayollar, bolalar, O'zbekiston, onlayn xavfsizlik qonuni, raqamli xizmatlar reglamenti

КИБЕРНАСИЛИЕ И ПРАВОВАЯ ЗАЩИТА: ОПЫТ УЗБЕКИСТАНА И ЕС

Хамраева Шахноза,

Специалист по социальным вопросам в международной консалтинговой компании «Juru»
E-mail: hamroyeva@gmail.com

Аннотация. Данная статья посвящена кибернасилию как растущей угрозе для женщин и детей. Анализируется законодательство Узбекистана и проводится сравнение с европейскими подходами к защите человека от онлайн-насилия, включая Закон Великобритании «О безопасности в Интернете» (2023 г.) и Регламент ЕС «О цифровых услугах» (2024 г.). В статье выявляются пробелы в национальном законодательстве, освещается международный опыт и предлагаются рекомендации по усилению защиты в цифровой среде Узбекистана.
Ключевые слова: кибернасилие, женщины, дети, Узбекистан, закон о безопасности в Интернете, закон о цифровых услугах.

Cyberviolence is a relatively new concept, so it doesn't yet have an internationally recognized definition. Various academic and legal sources describe it in different ways. By summarizing them, it can be understood that, cyberviolence is any act committed, assisted, aggravated or amplified by the use of information and communication technologies (mainly the Internet, mobile devices, social platforms) that violates the rights, dignity, online and offline well-being as well as the security of individuals.
It may take various forms, such as online harassment, which consists of bullying, sending threatening messages, and stalking; revenge porn, involving the distribution of sexually explicit images or videos without the consent of the person depicted; doxing, where an individual's personal information (such as their address and phone number) is released without their consent; hacking, which is unauthorized access to a person's computer on online accounts; identity theft, where an individual's personal information is appropriated by another for financial gain; sextortion, which involves the use of sexually explicit images or videos to blackmail the person depicted into providing money or other favors; cyber-stalking, wherein repeated harassment or threats take place via electronic communications; swatting whereby emergency services are tricked into responding to a fake emergency at a person's address; online impersonation, whereupon an individual pretends to be someone else in order to deceive or harm that

person,a d malware distribution, which constitutes the dissemination of malicious software to damage a system or steal personal information.[1]

At the national level, unfortunately, despite the widespread usage of the internet and social media platforms, very few aspects of it are regulated in the legislation of Uzbekistan. Certain aspects of cyberviolence are addressed in several legal documents. In 2019 two gender related legal acts were adopted by the Legislative Chamber:" On guarantees of equal rights and opportunities for women and men" and the Law "On Protection of Women against Harassment and Violence". The Law "On Protection of Women against Harassment and Violence" delineates four distinct types of violence: sexual, physical, economic, and psychological. Additionally, the law provides the issuance of protection orders for individuals affected by gender-based violence. These protective measures are promptly issued within 24 hours of establishing the occurrence of harassment, violence, or the threat thereof for a duration of up to thirty days.

With the Law No. 829 dated April 11, 2023, amendments were made to the Criminal Code of the Republic of Uzbekistan, criminalizing violence in the family. Law introduces the administrative and criminal liability for domestic violence and makes amendments to the Criminal Code and Administrative Liability Code accordingly. Moreover, the law extends the maximum term of protection orders from 30 days to 1 year. Besides, with this law, the term "stalking" was also introduced and included in the Law on "On Protection of Women against Harassment and Violence". According to the definition of stalking in the law, the term also includes cyberstalking.

Furthermore, some aspects of cyberviolence are regulated by the Criminal and Administrative liability Codes. Producing, importation, distribution, advertisement, demonstration of pornographic products as well as advertising, demonstration, distribution of pornographic products, including in the mass media, telecommunications networks or the world information network Internet (article 130 of the Criminal Code and article 189-1 of the Administrative liability Code), Slander or defamation, that is, the dissemination of deliberately false fabrications that disgrace another person in printed or otherwise reproduced form, including those posted in the media, telecommunications networks or the Internet (article 139 of the Criminal Code[2] and Article 40 of the Administrative liability Code[3]); Insult, that is, deliberate

[1] The roots of digital aggression: Exploring cyber-violence through a systematic literature review: Muaadh Mukred, Umi Asma' Mokhtar, Fahad Abdullah Moafa, Abdu Gumaei, Ali Safaa Sadiq, Abdulaleem Al-Othmani. Available at: https://doi.org/10.1016/j.jjimei.2024.100281

[2] The Criminal Code is available at: https://lex.uz/docs/111457

[3] The Administrative Liability Code is available at: https://lex.uz/docs/97661#203790

humiliation of the honor and dignity of a person in an indecent form, in printed or otherwise reproduced form, including posted in the media, telecommunications networks or the Internet (Art. 140 of the Criminal Code and art.41 of the Administrative liability Code); Violation of privacy - illegal collection or dissemination of information about the private life of a person, constituting his personal or family secret, without his consent (Article-141-1 of the Criminal Code and article -46-1 of the Administrative Liability Code); Disclosure of information that infringes on the honor and dignity of a person and reflects intimate aspects of a person's life that is distribution of information containing photos and (or) video images of a person's naked body and (or) genitals without his consent, including distribution in the media, telecommunications networks or the Internet, or the threat of dissemination of such information (Article 141-3 of the Criminal Code).

Besides, on 04/15/2022 the Law of Uzbekistan "On Cybersecurity"[4] was adopted. The law is mainly framework in nature and does not address specific measures to prevent cyberviolences, only by classifying responsibilities of government bodies in this field. There is no such term as "cyberviolence" or "cyber harassment" yet in the legislation of Uzbekistan.

According to the information published in the mass-media[5], Tashkent's Mirzo-Ulugbek District Criminal Court on 11th January, completed consideration of a criminal case against a group of people who created Telegram channels and groups called "Hello Tashkent, Salam Tashkent" in the messenger Telegram. Law enforcement agencies reported that the Telegram groups published intimate photos and videos of women, for the removal of which the group members demanded from 100,000 to 500,000 sums. They were found guilty with the following articles 130, 139, 140, 141-3, 165 of the Criminal Code. According to the Supreme Court website, almost all of the victims were women.

There exists, even more alarming situation concerning cyberviolence against adolescents, mainly young girls, which can lead to more critical consequences, if immediate actions are not taken to regulate the situation. Earlier the mass-media reported cyberbullying cases among schoolchildren, in Uzbekistan. Creators of the channel made fake photos of schoolboys, and mainly schoolgirls and demanded money for deleting them. Of course, this is not the only instance of cyber violence among the young people. The cases mentioned are just the ones that have been identified. When

[4] The text of the law is available at: https://lex.uz/ru/docs/5960609
[5] https://www.gazeta.uz/ru/2024/01/11/groups/?utm_source=push&utm_medium=telegram

young people witness such incidents or experience cyberbullying themselves, they often feel hesitant to openly discuss it or find themselves in a state of depression.

Before the acts of domestic violence were criminalized, almost nobody knew about the sufferings of the women and girls, or even if, somebody was aware of it, it was mostly ignored. This ignorance led to many suicides, and murders of many innocent women and girls. Therefore, any possibility of violation of rights must be deeply analyzed and measures must be taken to prevent them. Along with enhancing measures to prevent and combatt gender-based violence in our country, we shouldn't forget that other dangers and threats to human rights are arising. Especially in the technology era, most acute violations may take place in a very unnoticeable way. In this context, a question arises regarding the sufficiency of the law and bylaws in order to prevent and combat cyberviolence against women and girls. For this purpose, we have analyzed the European system of protecting human rights against cyberviolence, to compare our laws in this sphere with theirs and identify which aspects of them we can adopt in order to better prevent cyberviolence in our country.

It is important to note that the European system of protecting human rights against cyberviolence is one of the most developed in this field. The European Court of Human Rights, established in 1959, interprets the European Convention on Human Rights. The convention has had a huge impact on the law in Council of Europe member countries and is widely considered to be the most effective international treaty for human rights.[6] There has been a functioning the Court's Knowledge Sharing platform since 2022. It provides the latest analysis of case-law development in thematic and contextualized manner through Convention Articles. [7]

In the practice of the European Court of Human Rights there are several cases when the Court succeeded in establishing justice against cyberviolence towards women and girls.

One of them is the case of Buturuga v Romania which was reviewed by the Court in 2022. In this case, the woman, who had divorced her husband because of continuous domestic violence, sued Romania, which fails to investigate and prosecute her former husband, who after divorce, logged into her social network accounts and made copies of her private conversations, documents, and photos. Even though she files a complaint to the police against her husband, they didn't take it seriously by stating that it was not connected to the domestic violence complaint. The Court in Romania also didn't impose any punishment other than administrative fine, because of insufficient evidence

[6] European Convention for Human Rights Guide for the Civil and Public Service (Pdf) (Report). Irish Human Rights Commission.2012. ISBN 978-0-9569820-7-0.

[7] https://www.echr.coe.int/knowledge-sharing

and referring to the fact that the information that her husband copied were public. After that, the woman had to apply for protection order based on the national Law on preventing and combating domestic violence.

As a result, the Court found that there had been a violation of Articles 3 and 8[8] of the Convention, which prescribe that no one shall be subjected to torture or to inhuman or degrading treatment or punishment, and everyone has the right to respect for his private and family life, his home and his correspondence, on account of the failure to comply with the positive obligations arising from these provisions; and the respondent state was ordered to pay the applicant EUR 10,000 non-pecuniary damage and EUR 457 for costs and expenses. And the Court concludes that the national authorities did not approach the criminal investigation as raising the specific problem of domestic violence and that in doing so, they failed to give an appropriate response to the seriousness of the facts complained of by the applicant.

Besides having a good mechanism of protecting women through courts, several conventions were signed in the sphere of combating against gender-based violence. The Budapest, Lanzarote and Istanbul conventions emphasize the importance of criminalizing any conduct of violence against women and girls. Although, Istanbul Convention on preventing and combating violence against women and domestic violence doesn't specifically accentuate e online violence against women, its provisions can be applied to online violence as well. Furthermore, according to General Recommendations of GREVIO[9], the definition set out in Article 3a covers many forms of violence against women perpetrated online and the related requirements for state parties to establish legal and policy framework to tackle all forms of VAW should cover these forms cyber violence. Budapest convention was signed in 2001 for the purpose of regulating cybercrime in European countries, by harmonizing national laws and enhancing cooperation among nations. This convention includes measures related to computer-related fraud, copyright infringements, child pornography and network security breaches.

When it comes, to the Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, known as Lanzarote Convention, it lacks detailed measures for preserving electronic evidence in national and international

[8] Article 3 states that no one shall be subjected to torture and to inhuman or degrading treatment or punishment. And according to Article 8 Everyone has the right to respect for his private and family life, his home and his correspondence. Text of the convention is available at: https://www.echr.coe.int/documents/d/echr/Convention_ENG

[9] GREVIO (Expert group on action against violence against women and domestic violence) (2021), General Recommendation #1 on the digital dimension of violence against women, Council of Europe, Strasbourg, 20 October. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

inquiries concerning online sexual violence against children. Therefore, nations adopting these conventions should consider integrating the procedural powers of Articles 16 to 21 of Budapest Convention into their national legislations. By doing so, parties could enhance international collaboration regarding electronic evidence to address online sexual violence against children.

Although, these conventions were adopted several years ago, and some of them don't specify the peculiarities of regulation of online violence, they show that, in order to effectively protect the rights of women and children in the digital world, it is very important to collaborate with other countries in this sphere, since the digital world has no boundaries as the physical world does.

One of the noteworthy acts, which was adopted in the UK in 2023, is the Online Safety Bill developed by the Department for Science, Innovation and Technology and Department for Digital, Culture and Sport. This relatively new regulatory framework applies to companies whose services host user-generated content or facilitate interaction between users, one or more of whom is based in the UK, as well as search engines. Services playing a functional role in enabling online activity will remain out of scope, as will business to business services.[10] Some scholars[11] have argued that the bill requires further research, since it may violate the freedom of using the internet and give a lot of power to the Communications regulator in the UK (Ofcom) in regulating it. Bill has several objectives. Firstly, it aims to protect users from illegal content. Although violating the rights of people by creating and disseminating information is already prohibited according to the legislation, the purpose of the bill is to impose an obligation on service providers to control the digital space and with a view to limiting the potential spread of illegal content.[12]

Not long after the Online Safety Bill was adopted, the European Union's Digital Services Act (DSA), which had been adopted in 2022, came into force since the February of 2024. It introduces obligations for large online platforms to remove illegal content. It applies to all intermediary services, even if they are based abroad but serve in the EU. Whereas, Online Safety Bill focuses on the harmfulness of content, even it is legal (especially in cases of contents for children such as self-harm encouragement),

[10] https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response#part-1-who-will-the-new-regulatory-framework-apply-to

[11] A critical review of the Online Safety Bill. Markus Trengove, Emre Kazim, Denise Almeida, Airlie Hilliard, Sara Zannone, Elizabeth Lomas. Patterns 3, August 12, 2022. Available at: https://www.cell.com/patterns/pdf/S2666-3899(22)00147-7.pdf

[12] A critical review of the Online Safety Bill. Markus Trengove, Emre Kazim, Denise Almeida, Airlie Hilliard, Sara Zannone, Elizabeth Lomas. Patterns 3, August 12, 2022. Available at: https://www.cell.com/patterns/pdf/S2666-3899(22)00147-7.pdf

Digital Services Act focuses only on illegal content as defined in EU/national law (e.g. unlawful image sharing, online stalking, child sexual abuse etc.) without creating new offences, but ensuring consistent removal procedures. Within the scope of Online Safety Bill, platforms must publish annual transparency reports with Ofcom approved standards, which investigates and penalizes the breaches, which may be fines up to 10% of global turnover, blocking orders, or even criminal liability for executives. According to Digital Services Act, fines may be up to 6% of global turnover. Criminal liabilities are not stipulated, but the platforms can be forced to change the designs of algorithms and services.

Based on the above, recommendations for the context of Uzbekistan to decrease cyberviolence especially against women and children are as follows:

- Conducting surveys across the country to identify which types are widespread among the population and criminalize them, based on the assessment results, keeping statistics of victims of online violence and analyzing it by gender. Based on the results of the analysis, introducing changes to the law that criminalize online behavior that causes harm to the rights of others;
- Incorporating the concept “cyberviolence against women and girls” into the Law "On Protection of Women against Harassment and Violence” and Criminal Code and Administrative Liability Code;
- Further studying the practices of Online Safety Bill and Digital Services Act adopted in Europe, and adapt them in the context of Uzbekistan.