
INTERNATIONAL LEGAL PERSPECTIVE ON ONLINE GENDERED HARASSMENT AND VIOLENCE

Dr. Sakshee Sharma, School of Law, UPES University, Dehradun

While ICT has unlocked the doors for human civilisation beyond which lies endless potential to learn, explore, connect, share, create, invent, and express, there is no denying that in the past decade we also have witnessed the entrapments of letting ICT engulf our lives. Our greater indulgence into cyberspace with each passing day, leaves us vulnerable to the exacerbated malicious nature of the cyberspace.¹ And it is no surprise to see once again, the marginalised and the weak, to be at the receiving end of what the dark side of cyberspace has to offer. Online sexual harassment, intimidation, rape threats, trolling, cyber stalking, non-consensual image sharing are only the tip of the iceberg when it comes to the victimisation of women and girls on the internet. At the other end of the continuum is a wide range of harms that have a direct causal link to the harms mentioned above. Denial to women, the equal digital rights to participate in social life, in public spheres, political discourse, economic opportunities, and to attain empowerment is what we find brewing under the surface. Unfortunately, almost all societies are afflicted with greater harm caused by gendered cyber harassment. In 2016, a study conducted by Norton Symantec revealed that 76% Australian Women under the age of 30 reported to have faced harassment online.² Another 2020 Global Survey conducted by The World Wide Web Foundation and the World Association of Girl Guides and Girl Scouts revealed that 52 % of women have experienced online abuse in the form of threatening messages, non-consensual sharing of private images, and sexual harassment.³ In yet another survey of 14,000 girls and young women, across 31 countries, conducted by Plan International in 2020 revealed that 58% of the girls reported having personally experienced some form of Online Gendered Harassment and Violence (OGHV) on social media platforms. In Europe, the percentage was 63%, 60% in Latin America, 58% in Asia-Pacific region, 54% in Africa, and

-
- ¹ Arundhati Biswas, *The Great Gender Glitch: Women and Online Violence*, India Matters, Observer Research Foundation, 2023, Available at: <https://www.orfonline.org/expert-speak/the-great-gender-glitch/>
- ² J.R. Vickery and T. Everbach, *The Persistence of Misogyny: From the Streets, to Our Screens, to the White House* in *MEDIATING MISOGYNY: GENDER, TECHNOLOGY, AND HARASSMENT*, (J.R.Vickery and T. Everbach eds. 53, 2018).
- ³ PLAN INTERNATIONAL, *Free to be Online? Girl's and Young Women's Experience of Online Harassment* (2020), Available at: <https://plan-international.org/uploads/2023/06/SOTWGR2020-CommsReport-edition2023-EN.pdf>

52% of girls harassed online in North America.⁴ In light of these alarming numbers, it becomes quite imperative to take a look at the legislative efforts being made across the globe to prevent such largescale misogynistic attacks from happening to women online. Thus, the objective of the following text is to explore the current state of affairs relating to international commitments to fight OGHV.

International law has quite an elaborate assemblage of international and regional human rights instruments which call for equal rights for women by proscribing discrimination of women on social, political, and economic fronts. Human rights instruments like the Universal Declaration of Human Rights, hereinafter UDHR; International Convention on Civil and Political Rights, hereinafter ICCPR; International Convention on Economic, Social, and Cultural rights, hereinafter ICESCR; in general, and Convention on the Elimination of All Forms of Discrimination against Women hereinafter CEDAW; the Declaration on the Elimination of Violence against Women; and the Beijing Declaration; in specific, guarantee the entire gamut of rights to women.⁵ However, these instruments predate the ICT revolution and thus require to be substantiated with newer instruments which address the issue of gender inequality and gender-based violence in the cyberspace. In order to paint a picture of the current international laws, that in general or specifically mandate the State to ascertain protection of women in cyberspace, the following segment enlists such developments:

1. SOFT LAW ADDRESSING ONLINE GENDERED HARASSMENT AND VIOLENCE:

- (i) The Secretary-general of the UN, in 2006, conducted an ‘in-depth study on all forms of violence against women’. It was this study, which first recognised that ICT can be potentially used to cause violence against women. It observed the need of making inquiries in the use of ICT in order to assess the new forms of abuse against women that can be perpetrated through ICT. The report also called upon the States to acknowledge that combatting violence against women is a moving target due to the evolving nature of violence, and to be ready to respond to these new forms of violence as they are recognised.⁶

⁴ *Supra* note 3, PLAN INTERNATIONAL, at 16.

⁵ UN Human Rights Council, *Report of the Special Rapporteur on Violence against Women, Its causes and Consequences on online violence against women and girls from a human rights perspective* A/HRC/38/47, 11 (2018), Available at: <https://digitallibrary.un.org/record/1641160?ln=en>.

⁶ United Nations General Assembly, *In-dept study on all forms of violence against women: Report of the Secretary-General*, 36 (2006), Available at: [https://www.un.org/womenwatch/daw/vaw/SGstudyvaw .htm](https://www.un.org/womenwatch/daw/vaw/SGstudyvaw.htm)

- (ii) In 2012, Human Rights Council resolution 20/8 on ‘The promotion, protection and enjoyment of human rights on the internet’ referred to the rapid growth in the use of ICT by individuals across the globe. The resolution confirmed that this swift development in the use of ICT, warrants that the rights that people have offline, must also be protected online. The resolution made special reference to freedom of speech and expression found in Article 19 of UDHR and ICCPR.⁷
- (iii) The Commission on the Status of Women, in its 2013 report conclusions, agreed upon the important role that ICT and social media can play in the upliftment and empowerment of women and girls. In the same line of thought, the report also lay emphasis on the importance of developing combat mechanisms to prevent ICT facilitated violence against women and girls like cyberstalking and privacy violations that compromise the safety of women and girls.⁸
- (iv) In 2013, resolution 68/181 of the General Assembly on ‘Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognised Human Rights and Fundamental Freedoms: protecting women human rights defenders’, made several references to the online harassment and violence that the women human rights defenders have to face. The resolution called upon the States to create effective mechanisms to combat ICT related violations, abuses, discrimination, and violence against women including women human rights defender, to contain the proliferation of systematic gender-based discrimination against women.⁹
- (v) UN General Assembly 2016 resolution 71/199 on ‘The right to privacy in the digital age’¹⁰ and Human Rights Council’s 2017 resolution 34/7¹¹, noted that the infringement of right to privacy of individuals in the digital age, may particularly be experienced in an enhanced magnitude by women owing to their marginalised status. Thus, the resolutions called upon the States to

⁷ United Nations General Assembly, *Human Rights Council resolution 20/8 the promotion, protection and enjoyment of human rights on the internet*, 2 (2012), Available at: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

⁸ Commission on the Status of Women, *Report on the fifty-seventh session (2013)*, Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/277/44/PDF/N1327744.pdf?OpenElement>

⁹ United Nations General Assembly, *Resolution 68/181 Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognised Human Rights and Fundamental Freedoms: protecting women human rights defenders*. 2 (2015), Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/450/31/PDF/N1345031.pdf?OpenElement>

¹⁰ United Nations General Assembly, *Resolution 71/199 The right to privacy in the digital age* (2016).

¹¹ Human Rights Council, *Resolution 34/7 The right to privacy in the digital age* (2017), Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement>

develop preventive measures and remedies for violations of right to privacy which may be used effectively by women to mitigate the effects of such violations.

- (vi) The 2018 Resolution 38/5, adopted by the UN Human Rights Council concerned itself with the expeditious eradication of violence against women and girls, especially in the digital realm. Although, the Resolution lacks legal enforceability, its adoption is indicative of a political dedication from States, of their willingness to adopt a comprehensive strategy to address the digital violence faced by women and girls. These strategic measures typically should rely strongly on anti-discriminatory policies, which in turn would help enhance women's participation in, and access to the development of digital technologies. The Resolution, additionally, acknowledges the responsibility of business enterprises in addressing this issue.¹²
- (vii) The report of the UN Secretary-general in 2022 titled 'Intensification of efforts to eliminate all forms of violence against women and girls'¹³ dedicatedly addressed the growing concern of violence and sexual harassment of women and girls in the digital context, especially on social media. The report suggests that digital violence against women and girls is a part of a continuum that is connected to gender-based offline violence. It also acknowledges the enhanced impact of online violence, specifically on women's full and equal participation in public life. The report mentions the proliferation of new forms of OGHV due to artificial intelligence such as deepfakes pornographic videos, and its chilling impact of the personal and professional lives of women. The major contribution of the report in furthering the discussion on the issue, was the recognition of 'absence of agreed definitions and methodologies for measurement coupled with widespread underreporting' as the preliminary obstacles in assessing the actual prevalence of OGHV.

2. INTERNATIONAL HUMAN RIGHTS LAW RELATED TO ONLINE GENDERED HARASSMENT AND VIOLENCE

2.1 Right to Life- Freedom from Gender-Based Violence

As mentioned earlier, the international human rights instruments protecting the rights of

¹² Human Rights Council, *Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts*, Resolution 38/5 (2018), Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/214/82/PDF/G1821482.pdf?OpenElement>

¹³ U.N. Secretary-General, *Intensification of Efforts To Eliminate All Forms Of Violence Against Women And Girls* (2022), Available at: <https://documents-ddsny.un.org/doc/UNDOC/GEN/N22/465/68/PDF/N2246568.pdf?OpenElement>

women against gender-based violence, predates the digital era and thus do not specifically include the mention of gender-based violence perpetrated in cyberspace. However, these instruments have been continuously analysed and recommendations have been produced to the States to interpret these instruments to be applicable even to online violence and abuse. While the Committee on the Elimination of Discrimination against Women had first made a reference to the digital dimension of violence against women in State reports of 2016, it was in its general recommendation No. 35 (2017) on CEDAW that it clearly implied that the Convention's applicability extends to technology-mediated environments such as the internet and digital spaces, which have become platforms of frequent violence against women and girls in its digitalised form. Additionally, the committee recommended to the State parties to regularly collect, analyse and publish data on the complaints regarding all forms of gender-based violence including the technology-mediated violence.¹⁴

2.2 Freedom of Expression

Article 19 of UDHR and ICCPR, enshrine upon individuals, the right to freely express their opinions and ideas through any media of their choice. The term 'any media' as interpreted in today's context is wide enough to include within its ambit digital spaces as well. Thus, individuals, irrespective of their gender, have the right to exercise their right to freedom of expression even in cyberspace. The UN Special Rapporteur report mentioned that online gender-based abuse and violence assail the fundamental principles of equality and freedom of expression, thus recognising women's right to expression in cyberspace as a part of the core principles of human rights.¹⁵

2.3 Right to Privacy and Data Protection

Article 12 of the UDHR and article 17 of the ICCPR unequivocally recognise the right to privacy as an inalienable right within the spectrum of human rights. When looked in the context of right to privacy, most forms of online gender-based violence are committed by infringing upon the privacy of women. Cyberstalking, sextortion, non-consensual dissemination of

¹⁴ United Nations Committee on the Elimination of Discrimination against Women, *General recommendation No. 35 on gender-based violence against women*, 18 (2017), Available at: https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Download.aspx?symbolno=CEDAW/C/GC/35&Lang=en

¹⁵ *Supra* note 5.

intimate images, doxing, cyber hate, etc. are all harms that either result into or are results of violation of right to privacy.¹⁶

3. INTERNATIONAL CONVENTIONS RELATED TO ONLINE GENDERED HARASSMENT AND VIOLENCE

3.1 Budapest Convention 2001

The changes brought about by the rapid digitalisation and globalisation of computer networks and the increasing need of international cooperation to fight cybercrimes led to the drafting and adoption of the first and only binding convention on the subject matter.¹⁷ The Council of Europe Convention of Cybercrime popularly known as Budapest Convention was adopted in 2001, came into force in 2004 and currently has sixty-eight State parties to it. The Convention of Cybercrimes (COC) mandates the governments to combat cybercrimes by criminalising certain conducts, and to detect, investigate and prosecute them at both domestic and international levels.¹⁸ The convention was preceded by a few attempts at the international level, which concerned themselves with crimes against computer and ICT, like the International droit Pone Conference in Germany (1992), Twenty-Second G-7 Summit on Cyber Crime (1996), G-8 High-Tech Crime Working Group (1998), Paris Cyber Crime Conference (2000) and Internet Treaty by Council of Europe (2001)¹⁹, but it was the Budapest convention that tried to address the challenges that cybercrimes raised for the traditional criminal law and justice system. The Convention, while not attempting to define 'cybercrime', classified them into four groups based on the characteristics of the offences: 1. offences against the confidentiality, integrity and availability of data and information system, 2. computer related offences, 3. content related offences, 4. Infringement of copyright. The Convention in articles 2-11 calls for criminalisation of nine offences, including illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related fraud and forgery,

¹⁶ ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS, *Providing a gender lens in the digital age: APC submission to the office of the High Commissioner for Human Rights' Working Group on Business and Human Rights*, 10 (2018), Available at: <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Gender/APC.pdf>

¹⁷ Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425-429 (2003).

¹⁸ The Council of Europe Convention on Cybercrimes, 2001, Preamble, Available at: <https://rm.coe.int/1680081561>.

¹⁹ Kamshad Mohsin, *Global Perspective of Cyber Crimes and Related Laws*, SSRN ELECTRONIC JOURNAL, (2020), Available at: https://www.researchgate.net/publication/346020153_Global_Perspective_of_Cyber_Crimes_and_Related_Laws

dissemination of racist or xenophobic material, dissemination of child pornography, and copyright violations.²⁰ Articles 16-21, enlists certain investigative and legislative measures that may be necessary for prevention of and protection against the offences listed in the convention.

However, when looked at through the lens of gender, the Convention is oft criticised to provide no protection to women whatsoever, rendering it largely ineffective to be used for the protection of women against online gender-based violence. Neither does the Convention incorporate any provision relating to gender specific offences which are particularly targeted against women, nor does it contain offences wide enough to include within their ambit, all forms of cyber harassment. Many of the nine offences mentioned above, does not include within their domain behaviours like cyber stalking or revenge pornography, thus futile for the victims of cyber harassment.²¹ The closest the Convention came to including gender-based cybercrimes was in Art 14 (b), where it states that the mandate on the States to introduce new investigative powers and procedural rules, not only apply for the offences mentioned in the Convention, but also to ‘other criminal offences committed by means of a computer system’.²²

3.2 Istanbul Convention, 2011

Council of Europe’s Convention on Preventing and Combating Violence against Women and Domestic Violence, popularly known as Istanbul Convention is an important human rights treaty which establishes comprehensive legal standards for women’s rights against gender-based violence. The Convention acknowledges that violence against women in its different forms is a manifestation of the historically imbalanced power equation between men and women, and that the perpetuation of such violence is further going to impair the situation.²³

The Convention in article 3, defines ‘violence against women’ as ‘a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological, or economic harm, or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty,

²⁰ Amalie M. Weber, *The Council of Europe’s Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 431 (2003).

²¹ *Id.*, at 435-436.

²² The Council of Europe Convention of Cybercrime, 2001 [hereinafter Budapest Convention, 2001, Article 14.

²³ Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence, 2011, [hereinafter Istanbul Convention, 2011], Preamble, *Available at*: <https://rm.coe.int/168008482e>

whether occurring in public or in private life'.²⁴ The Convention lays out a mandate for the State parties to ensure fundamental rights of equality and non-discrimination to women through appropriate legislative measures²⁵, and incorporate gender sensitive policies ensuring women empowerment.²⁶

However, the Istanbul Convention, 2011 does not expressly address violence against women perpetrated in online spaces despite coming into force in relatively recent past (2014). The Explanatory Report to the Convention, for the most part remains silent on the matter, except for a lone mention of 'online stalking'.²⁷ The Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) was set up as a monitoring body for the implementation of the convention in 2015. Recently in 2021, GREVIO in its first General Recommendation on the Digital Dimension of Violence Against Women, expanded on the Explanatory Report by setting out the domain of the Convention to include online and technology-facilitated violence against women by stating that the term 'digital dimension of violence against women' encompass both online and technology facilitated harmful behaviour against women.²⁸ Thus, the General Recommendation can be viewed as an attempt by GREVIO to fill the normative gap that was left in the Convention during its drafting.

CONCLUSION

The study of online gendered harassment and violence (OGHV) has revealed the pressing need for robust legal, institutional, and societal mechanisms to address the alarming rise of such behaviour globally. In an era where information and communication technologies (ICTs) permeate every facet of human interaction, the dual nature of cyberspace—as a tool for empowerment and a weapon for abuse—has become increasingly apparent. This duality demands a nuanced understanding of how gendered violence manifests in digital spaces and the specific vulnerabilities it exploits.

Unfortunately, the elaborate international legal framework that extensively acknowledges

²⁴ Istanbul Convention 2011, Article 3(a), Available at: <https://rm.coe.int/168008482e>

²⁵ Istanbul Convention 2011, Article 4, Available at: <https://rm.coe.int/168008482e>

²⁶ Istanbul Convention 2011, Article 6, Available at: <https://rm.coe.int/168008482e>

²⁷ Council of Europe, *The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform*, 16 (2022), Available at: https://www.ohchr.org/sites/default/files/documents/hrbodies/cedaw/statements/2022-12-02/EDVAW-Platform-thematic-paper-on-the-digital-dimension-of-VAW_English.pdf

²⁸ *Supra* note 27.

women's rights, is found to be ineffective to address the realities of technology assisted gendered abuses. Owing to their origins in the pre-digital era, instruments like UDHR, ICCPR, ICESCR, CEDAW etc. often fall short of catering to the victims of OGHV. Due to an absence of specific provisions catering to digital violence targeted towards marginalised populations, one of them being women, their applicability in such instances can only be through a patchwork of interpretations, non-binding resolutions, and supplementary mechanisms to fill the cracks between principle and practice.

The existing significant international instruments on crimes occurring in cyberspace i.e. the Budapest Convention of 2001, and violence against women i.e. the Istanbul Convention of 2011, too have exhibited limitations in comprehensively combatting OGHV. The absence of different forms of OGHV like cyberstalking and revenge pornography from the Budapest Convention and the omission of the mention of digital aspect of gendered violence in the original text of the Istanbul Convention, greatly reflects on the oversight of these grave issues by the international community. While efforts like GREVIO's 2021 general recommendation to address the digital dimension of violence against women are commendable, they remain non-binding, leaving implementation to the discretion of individual states.

Soft law instruments, including UN General Assembly resolutions and Human Rights Council reports, have highlighted the growing menace of digital violence. However, these instruments often lack enforceability, reducing their efficacy in compelling state action. The absence of standardized definitions, data collection methodologies, and comprehensive metrics further hampers global efforts to combat OGHV effectively. Without a unified approach, the fight against online gendered violence risks remaining fragmented and inconsistent.

Research has also indicated a great level of the intersectionality of online abuse and violence, with women from marginalized communities, including LGBTQ+ individuals, ethnic minorities, and economically disadvantaged groups, facing compounded vulnerabilities and enhanced victimisation. The global nature of the internet coupled with eased and cheap accessibility means that cultural and societal norms influencing gender-based violence in one region can easily transmute across digital spaces, creating a complex, borderless challenge for regulators and activists alike.

The findings bring to light the urgency to implement multifaceted approach to combating OGHV. Legislative reforms at the national and international levels prioritising gender-sensitive

policies, explicitly addressing the unique challenges posed by digital violence can be a good starting point. International instruments like the CEDAW Committee's General Recommendation No. 35 on gender-based violence provide a valuable precedent for interpreting existing laws to include online violence. However, these interpretations must be codified into enforceable obligations for state parties, ensuring uniformity in their application.

Moreover, the role of technology companies cannot be overstated. Platforms must adopt proactive measures to prevent and mitigate OGHV, including transparent moderation policies, enhanced reporting mechanisms, and user education. Governments should collaborate with these entities to ensure compliance with regulatory frameworks while balancing freedom of expression with the need to protect vulnerable populations.

Education and awareness campaigns targeting both men and women are equally critical. Empowering individuals with digital literacy and self-protection tools can mitigate their exposure to online risks. Simultaneously, fostering a culture of accountability through public discourse and advocacy can challenge the normalization of gendered abuse online.