Page 1455 - 1467 **DOI:** *https://doi.org/10.63108/IJLMH.13323*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Digital Gender-Based Violence in the Age of Artificial Intelligence

KOSTURIKA BANDYOPADHYAY*

ABSTRACT

Technology has increased and changed the gender-based violence (GBV) faced by women and girls globally. This paper explores the ways in which AI technology causes GBV and evaluates whether current laws address the issue, with a specific focus on India. Four forms of GBV are identified. AI is used to spread disinformation, increasing the vulnerability of women in conflict zones. Deepfake technology is overwhelmingly used to create non-consensual pornography and to silence women in the media and public life. Biometric and facial recognition data are collected and used, for example from Rohingya refugees, and to monitor whether women in Iran are wearing the hijab as required. Women activists are targeted through cyberstalking, defamation and de-platforming. The international framework includes General Recommendations No. 19 and No. 35 of the CEDAW Committee, the Istanbul Convention and Council of Europe standards on sexist hate speech. Within India, the Information Technology Act, 2000, the IT Intermediary Rules, 2021 and the Bharatiya Nyaya Sanhita, 2023 address the issue. However, although these laws have been extended to cover technology-facilitated GBV, and the Intermediary Rules were amended in 2026 to address synthetically generated content, there is still no law dealing specifically and fully with AI-facilitated GBV. Regulation of AI and protection of gender equality continue to develop separately, so the accountability of platforms and developers is lacking. To improve this, the two can be combined through measures such as safety by design, labelling of deepfakes, red-teaming, clear processes for escalating the cases of vulnerable women, protection for whistleblowers and digital education. National laws need strengthening, institutional capacity should be improved, and societal attitudes towards women in digital spaces must change. Globally, AI needs to be regulated with a focus on protecting women's rights, particularly in countries where authoritarian systems deploy AI surveillance.

Keywords: *Digital gender-based violence, Artificial intelligence, Deepfakes, Cyberstalking*

I. INTRODUCTION

Gender-based violence (GBV) is a pervasive issue affecting women and girls worldwide, manifesting in various forms across physical and digital spaces. In the twenty-first century,

* Author is a PhD Scholar at National Law University, Delhi, India. ORCID: https://orcid.org/0009-0004-6662-1835

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

advances in technology, ranging from mobile devices to sophisticated tools such as artificial intelligence (AI), have dramatically altered how GBV is both perpetrated and addressed. Technologies initially developed for efficiency and communication have also enabled new forms of harassment, creating complex security concerns in cyberspace.

A prominent example of the threats posed by technology is the 2014 attack that leaked private photographs of numerous female celebrities. Hackers gained access to the victims' Apple iCloud accounts, and the intimate images obtained were posted online and went viral.[1] The incident illustrates how women are disproportionately targeted by cyberattacks, which range from privacy breaches to online harassment, including revenge porn, cyberstalking and cyberbullying.[2] Such attacks can be exacerbated by AI and other automated tools that facilitate the rapid distribution of harmful content, intensifying the impact on victims. The availability of personal information online, through social media geotagging and other digital tracking tools, has further escalated risks such as cyberstalking, creating safety concerns not only in digital spaces but also in real-life settings.

The rise of AI represents a new chapter in technology's influence on GBV. AI tools, including chatbots and recommendation algorithms, can contribute to the spread of GBV-related content by amplifying harmful material or enabling harassment at a larger scale. As technology continues to develop, it becomes essential for those involved in GBV response and prevention to understand how different types of AI might affect GBV, either by contributing to it or by offering innovative solutions to combat it.[3]

Addressing GBV in the digital age requires an understanding of fundamental concepts related to AI and its applications. Artificial intelligence broadly refers to the use of computational methods, such as machine learning (ML) and deep learning, to process large datasets and enable intelligent problem-solving. AI relies on algorithms, or specific sets of rules that machines can execute, to perform complex tasks such as pattern recognition, text analysis and image processing, as well as generating speech that mimics human communication. AI also incorporates capabilities such as natural language processing (NLP), knowledge representation and automated reasoning, all of which allow it to simulate human-like behaviour. Some AI applications, such as chatbots, exist solely in virtual domains, while others are integrated into

[1] Melissa Chan, *Pennsylvania Man Charged in Celebrity Nude Photos Hacking Scheme*, TIME (Mar. 15, 2016), https://time.com/4260056/celebrity-nude-photo-hack-arrest-celebgate/ (last visited Nov. 22, 2026).

[2] Khalil Goga, *How to Tackle Gender-Based Violence Online*, WORLD ECON. F. (Feb. 18, 2015), https://www.weforum.org/agenda/2015/02/how-to-tackle-gender-based-violence-online/.

[3] Jeanne Ward, Sarah Spencer & Kavita Kalsi, *Gender-Based Violence and Artificial Intelligence (AI): Opportunities and Risks for Women and Girls in Humanitarian Settings* (GBV AoR Helpdesk, Aug. 2023), https://gbvaor.net/node/1903 (last visited Nov. 22, 2026).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

the Internet of Things (IoT), which connects them to physical devices and allows AI to interact with the real world in diverse and far-reaching ways.

As AI technologies continue to evolve, their role in both perpetuating and addressing GBV becomes increasingly significant. On the one hand, AI-driven platforms may facilitate GBV through unchecked algorithms and automated processes that inadvertently propagate harmful behaviour. On the other hand, AI offers innovative tools that, if ethically developed and carefully regulated, can support efforts to prevent and respond to digital GBV. As the landscape of technology-facilitated violence shifts, continuous research, public awareness and policy development are crucial to ensuring that AI serves as a force for protection rather than harm.

II. Forms of Digital Gender-Based Violence in the Age of AI

The rapid rise of AI presents new and significant risks for women and girls, especially those in vulnerable and marginalised settings. AI-facilitated digital GBV manifests in various ways, from AI-driven disinformation to the use of deepfakes and advanced biometrics for surveillance and tracking, all of which expose women and girls to targeted harassment and increased security risks. This part examines the multifaceted nature of digital GBV enabled by AI, and how technological advances have created both opportunities for empowerment and channels for violence, harassment and the discrediting of women.

A. Disinformation

One form of AI-driven GBV is disinformation, which can be intentionally created and amplified by AI to deceive, manipulate or incite violence. The European Commission defines disinformation as "false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm".[4] AI can fuel disinformation in two primary ways: by generating false content, and by amplifying its reach through social media algorithms. Disinformation has been weaponised by state and non-state actors in various countries to incite racial, ethnic and religious violence. In Myanmar, for instance, Amnesty International found that the algorithms of Meta's Facebook platform amplified content inciting violence against the Rohingya, contributing to the atrocities committed against them, including mob violence, rape and ethnic cleansing.[5] In such conflicts, women and girls are particularly vulnerable to conflict-related sexual violence and other forms

[4] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan*, at 18, COM (2020) 790 final (Dec. 3, 2020).

[5] Amnesty Int'l, *Myanmar: The Social Atrocity: Meta and the Right to Remedy for the Rohingya*, AI Index ASA 16/5933/2022 (Sept. 29, 2022), https://www.amnesty.org/en/documents/asa16/5933/2022/en/ (last visited Nov. 22, 2026).

of GBV, which can escalate when women are forced to flee or are displaced, increasing the risks of intimate partner violence, sexual assault and exploitation in refugee settings.

B. Deepfakes

Deepfakes, AI-generated synthetic media that produce highly realistic but fake images, videos or audio, constitute another concerning form of digital GBV. Deepfake technology has made it easier to create falsified content without extensive training data, leading to its misuse in disinformation campaigns and targeted harassment.[6] Deepfakes are often used to create non-consensual pornographic videos: one industry study found that 98 per cent of deepfake videos online are pornographic and that 99 per cent of the individuals targeted in deepfake pornography are women.[7] Female public figures, journalists and activists are particularly targeted, as the case of the Indian journalist Rana Ayyub, against whom a deepfake was made and circulated on social media in 2018, shows.[8] Deepfakes not only undermine the credibility of the affected individuals but also contribute to a chilling effect on women's freedom of expression, as they risk facing public backlash and defamation. This was highlighted during the 2023 Slovak parliamentary election campaign, when, two days before the vote, a fabricated video carrying AI-generated audio of a journalist and a party chairman discussing electoral fraud circulated on social networks, in what press freedom groups described as one of the first such uses of the technology in the European Union.[9]

C. Surveillance

In addition to disinformation and deepfakes, AI-powered biometric surveillance has emerged as a growing threat to women in humanitarian settings. AI-enabled biometrics can track individuals on the basis of physiological and behavioural traits, making them a tool for verifying identities and facilitating aid distribution in conflict zones. If biometric data are mishandled, however, they can put women and girls at heightened risk. Since 2018, for instance, the Office of the United Nations High Commissioner for Refugees (UNHCR) has registered Rohingya

---

[6] Eleonore Pauwels, *Artificial Intelligence and Data Capture Technologies in Violence and Conflict Prevention* 13 (Global Ctr. on Coop. Sec. Policy Brief, Sept. 2020), http://www.jstor.org/stable/resrep27551 (last visited Nov. 22, 2026).

[7] SECURITY HERO, *2023 State of Deepfakes: Realities, Threats, and Impact* (2023), https://www.homesecurityheroes.com/state-of-deepfakes/ (last visited Nov. 22, 2026); Rangita de Silva de Alwis & Elodie Vialle, *Is AI-Facilitated Gender-Based Violence the Next Pandemic?*, REGUL. REV. (May 6, 2024), https://www.theregreview.org/2024/05/06/de-silva-de-alwis-vialle-is-ai-facilitated-gender-based-violence-the-next-pandemic/ (last visited Nov. 22, 2026).

[8] Sophie Compton, *What Are Deepfakes? More and More Women Are Facing This Form of Online Abuse*, VOGUE (Mar. 16, 2021), https://www.vogue.com/article/scary-reality-of-deepfakes-online-abuse (last visited Nov. 22, 2026).

[9] Karin Kőváry Sólymos, *Slovakia: Deepfake Audio of Denník N Journalist Offers Worrying Example of AI Abuse*, INT'L PRESS INST. (Oct. 31, 2023), https://ipi.media/slovakia-deepfake-audio-of-dennik-n-journalist-offers-worrying-example-of-ai-abuse/ (last visited Nov. 22, 2026); De Silva de Alwis & Vialle, *supra* note 7.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

refugees in Bangladesh, collecting photographs, fingerprints and other biometric and biographic data, and the Bangladesh government has shared this information with the Myanmar government to verify people for possible repatriation, raising concerns about reprisals against returnees.[10] For women and girls, such exposure may also heighten the risk of GBV. Even beyond humanitarian settings, biometric data could be exploited by government authorities or unauthorised entities to surveil and target women, leaving them vulnerable to GBV.

AI systems are also increasingly being used to target women disproportionately, allowing authorities to exert more control over their movements, which is particularly troubling in authoritarian regimes. In 2022, for example, Iranian authorities announced plans to use facial recognition technology on public transport to identify women not complying with strict hijab rules. Commentators have read the move as a political statement rather than a mere technical choice. The systems draw on Iran's extensive information infrastructure, which links citizens' profiles to a national biometric database containing vast amounts of personal data. This surveillance network, combining traditional state control with advanced AI capabilities, shows the growing complexity of enforcement mechanisms, especially where women's rights are directly affected.[11]

D. Targeting female activists and vulnerable women and girls

The rise of cyberstalking, harassment and cyber defamation exacerbates these risks. As more women engage with digital spaces to express opinions and advocate on social issues, they face an increase in technology-mediated violence, including cyberstalking, defamation, email spoofing and psychological abuse. Cyberstalking extends traditional stalking through digital tools, as perpetrators repeatedly harass or threaten women through online platforms. Cyber defamation in particular has become a potent tool for damaging the reputation of women, since false content can be spread rapidly and accessed by a large audience with minimal effort. Anonymity on digital platforms can embolden perpetrators. Indian law reaches cyberstalking through the offence of stalking in section 78 of the Bharatiya Nyaya Sanhita, 2023,[12] online

[10] HUM. RTS. WATCH, *UN Shared Rohingya Data Without Informed Consent* (June 15, 2021), https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent (last visited Nov. 22, 2026).

[11] Weronika Strzyżyńska, *Iranian Authorities Plan to Use Facial Recognition to Enforce New Hijab Law*, GUARDIAN (Sept. 5, 2022), https://www.theguardian.com/global-development/2022/sep/05/iran-government-facial-recognition-technology-hijab-law-crackdown (last visited Nov. 22, 2026); Maria Beatriz Saboya, *Surveillance, Identity, and Gender: Navigating the AI-Driven Digital Age*, DIGIT. CONSTITUTIONALIST, https://digi-con.org/surveillance-identity-and-gender-navigating-the-ai-driven-digital-age/ (last visited Nov. 22, 2026).

[12] The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, § 78 (India) [hereinafter BNS].

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

defamation through section 356,[13] and online threats through the offence of criminal intimidation in section 351,[14] yet enforcement remains challenging.

Digital GBV also affects women's access to public discourse. Online violence against women journalists, activists and human rights defenders can lead to the "de-platforming" of women's voices, creating a chilling effect on freedom of expression and democratic dialogue. This suppression of women's voices aligns with trends of digital authoritarianism, in which anti-feminist narratives are wielded to justify the oppression of marginalised groups.[15] The proliferation of AI-driven online violence, including disinformation, deepfakes and cyber harassment, reflects how technology can be weaponised against women, intensifying existing forms of gender-based violence in the digital age.

III. Legal frameworks and AI's role in addressing digital GBV

A. International framework

GBV in cyberspace is a growing global concern, exacerbated by rapid advances in information and communication technology (ICT). Definitions of gender-based violence and cybercrime nevertheless struggle to capture the full nature and scope of cyber-related gender violence. Numerous international organisations and treaties have made significant strides in defining, addressing and curbing violence against women in digital spaces, creating a framework for international cooperation and legal action.

Two general recommendations of the UN Committee on the Elimination of Discrimination against Women (CEDAW Committee) are relevant:

- General Recommendation No. 19 defines gender-based violence as violence that is directed against a woman because she is a woman or that affects women disproportionately. The definition includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty.[16]
- General Recommendation No. 35 updates General Recommendation No. 19 and extends it to technology-mediated environments. It recognises that gender-based violence against women occurs in all spaces and spheres of human interaction, public and private, including through the redefinition of public and private by technology-

[13] BNS, *supra* note 12, § 356.
[14] *Id.* § 351.
[15] De Silva de Alwis & Vialle, *supra* note 7.
[16] Comm. on the Elimination of Discrimination Against Women, *General Recommendation No. 19: Violence Against Women*, ¶ 6, U.N. Doc. A/47/38 (1992), https://www.un.org/womenwatch/daw/cedaw/recommendations/index.html (last visited Nov. 22, 2026).

mediated environments, such as contemporary forms of violence occurring online and in other digital environments.[17]

The UN General Assembly resolution on the Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: Protecting Women Human Rights Defenders addresses technology-related abuses against women human rights defenders, including online harassment, cyberstalking, violation of privacy, censorship and the hacking of e-mail accounts, mobile phones and other electronic devices. It recognises that such acts, used to discredit women defenders or to incite further abuses against them, are a growing concern and can be a manifestation of systemic gender-based discrimination.[18]

In a 2018 report to the Human Rights Council, the Special Rapporteur on violence against women, its causes and consequences defined online violence against women as any act of gender-based violence that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the internet, social media platforms or email. The report acknowledges the evolving nature of online violence and notes that the rapid development of digital technology, including AI, will inevitably give rise to new manifestations of violence against women.[19]

The Council of Europe's Istanbul Convention, which GREVIO, the expert body that monitors it, describes as the most far-reaching treaty in its field, sets legally binding standards for preventing and combating violence against women. It contains no provision written specifically for online conduct, but GREVIO has confirmed that several of its articles reach violence committed through digital means.[20]

- Article 3(a) defines violence against women as a violation of human rights and a form of discrimination against women, covering all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm,

---

[17] Comm. on the Elimination of Discrimination Against Women, *General Recommendation No. 35 on Gender-Based Violence Against Women, Updating General Recommendation No. 19*, ¶ 20, U.N. Doc. CEDAW/C/GC/35 (July 26, 2017), https://undocs.org/CEDAW/C/GC/35.

[18] G.A. Res. 68/181, pmbl. (Dec. 18, 2013), https://undocs.org/A/RES/68/181.

[19] Special Rapporteur on Violence Against Women, Its Causes and Consequences, *Report on Online Violence Against Women and Girls from a Human Rights Perspective*, ¶¶ 23–24, U.N. Doc. A/HRC/38/47 (June 18, 2018), https://undocs.org/A/HRC/38/47.

[20] Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence, May 11, 2011, C.E.T.S. No. 210, https://www.coe.int/en/web/istanbul-convention/text-of-the-convention [hereinafter Istanbul Convention]; GRP. OF EXPERTS ON ACTION AGAINST VIOLENCE AGAINST WOMEN & DOMESTIC VIOLENCE (GREVIO), *General Recommendation No. 1 on the Digital Dimension of Violence Against Women* ¶ 8 (Oct. 20, 2021), https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147 [hereinafter GREVIO Recommendation].

whether occurring in public or in private life. According to GREVIO, this definition covers violence perpetrated against women through digital means.[21]

- Article 3(b) defines domestic violence to include violence between former or current spouses or partners, whether or not they share a residence, which may extend to online harassment or abuse by current or former partners, reflecting the Convention's holistic approach to GBV across all settings.[22]
- Article 33 requires the criminalisation of psychological violence, the intentional conduct of seriously impairing a person's psychological integrity through coercion or threats, which GREVIO considers applicable to online harassment.[23]
- Article 34 requires the criminalisation of stalking, the intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety, which includes stalking committed through ICT.[24]
- Article 40 covers sexual harassment, defined as any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, which can include sexually explicit messages or unwanted advances in cyberspace.[25]

The Council of Europe's Additional Protocol to the Convention on Cybercrime is confined to acts of a racist and xenophobic nature committed through computer systems.[26] The definition of sexist hate speech comes instead from the Council's work on gender equality, which describes it as including "expressions which spread, incite, promote or justify hatred based on sex", and the Committee of Ministers, in its 2019 Recommendation on preventing and combating sexism, has called on member States to define and criminalise sexist hate speech in all media, providing a foundation for addressing gender-based hate speech in cyberspace.[27]

The international framework for combating violence against women in cyberspace reflects a growing recognition of the distinctive challenges posed by ICT-facilitated abuse. These frameworks, although varied in scope and application, collectively emphasise the need for strong, responsive measures to protect women from digital forms of GBV. While considerable

[21] Istanbul Convention, *supra* note 20, art. 3(a); GREVIO Recommendation, *supra* note 20, ¶ 33.
[22] Istanbul Convention, *supra* note 20, art. 3(b); GREVIO Recommendation, *supra* note 20, ¶¶ 25, 43.
[23] Istanbul Convention, *supra* note 20, art. 33; GREVIO Recommendation, *supra* note 20, ¶¶ 36, 42–43.
[24] Istanbul Convention, *supra* note 20, art. 34; GREVIO Recommendation, *supra* note 20, ¶¶ 40–41.
[25] Istanbul Convention, *supra* note 20, art. 40; GREVIO Recommendation, *supra* note 20, ¶¶ 37–38.
[26] Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, Jan. 28, 2003, E.T.S. No. 189.
[27] COUNCIL OF EUROPE, *Combating Sexist Hate Speech* 2 (2016), https://rm.coe.int/1680651592; Comm. of Ministers, Council of Europe, *Recommendation CM/Rec(2019)1 on Preventing and Combating Sexism*, app. § II.B.1 (Mar. 27, 2019), https://rm.coe.int/cm-rec-2019-1-on-preventing-and-combating-sexism/168094d894.

progress has been made, continuing technological advances, especially in AI and ICT, will require continuous updating of these international standards to ensure comprehensive protection for women worldwide.

B. Indian framework

In India, recent legal developments target digital gender-based violence, which is particularly relevant in an era of AI. Although no specific law fully regulates AI-enabled gender-based abuse, existing frameworks have adapted to address these emerging threats.[28] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 require intermediaries to make reasonable efforts to ensure that users do not host or share content that is obscene, invasive of another's privacy, including bodily privacy, or insulting or harassing on the basis of gender, which can include AI-driven abuse such as deepfakes and the non-consensual sharing of intimate images.[29] On a complaint by the individual concerned, an intermediary must remove or disable access to content that exposes that individual's private area, shows the individual in full or partial nudity or in a sexual act, or impersonates the individual, including through artificially morphed images, within two hours of the complaint (twenty-four hours until February 2026). This has implications for tackling AI-generated content that violates privacy.[30]

Section 66E of the Information Technology Act, 2000 punishes intentionally or knowingly capturing, publishing or transmitting the image of a private area of any person without that person's consent, under circumstances violating privacy.[31] The provision addresses the non-consensual circulation of sexually explicit material.

Sections 67 and 67A punish publishing or transmitting, in electronic form, obscene material and material containing sexually explicit acts or conduct respectively. They reach such content when it is circulated through social media, blogs and other platforms, including trolling, and through email and messaging services, which is how sexually explicit images of a person are commonly spread without that person's consent and against their will.[32] Section 67B is an important

[28] NORC AT THE UNIV. OF CHI. & INT'L CTR. FOR RSCH. ON WOMEN, *Technology-Facilitated Gender-Based Violence in India* (USAID 2022), https://genderit.org/resources/technology-facilitated-gender-based-violence-india.
[29] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), r. 3(1)(b)(ii), Gazette of India, pt. II sec. 3(i) (Feb. 25, 2021) (India), as amended by G.S.R. 120(E) (Feb. 10, 2026) [hereinafter IT Rules].
[30] *Id.* r. 3(2)(b).
[31] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 66E (India).
[32] *Id.* §§ 67, 67A.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

provision that punishes publishing or transmitting material depicting children in sexually explicit acts, as well as creating, browsing, downloading or distributing such material.[33]

In addition, the Bharatiya Nyaya Sanhita, 2023 (BNS) contains provisions on harassment, stalking and defamation that can be applied to online abuse. Section 78 defines stalking to include a man monitoring a woman's use of the internet, email or any other form of electronic communication, which may involve AI-based tracking technologies.[34] Section 356 defines defamation, and can be invoked by women on social media or on blogs in cases of libel and slander.[35] Section 351 punishes criminal intimidation, and section 351(4) adds a further term of up to two years' imprisonment where the threat is made by anonymous communication or the sender conceals their identity, as is common in trolling and threats on social media.[36] Responding to concerns about deepfakes, the Intermediary Rules were amended with effect from 20 February 2026 to define "synthetically generated information" and to require intermediaries offering tools to create it to prevent the creation of unlawful synthetic content, including non-consensual intimate imagery, and to label the rest prominently.[37]

IV. Need for Legal and Ethical AI Reforms

Legislative efforts currently tend to address AI and gender issues separately, but there is an urgent need to recognise their intersection. The EU Artificial Intelligence Act[38] represents a groundbreaking move towards regulating AI, while the EU has also adopted a Directive on combating violence against women and domestic violence, which covers physical, sexual, psychological and economic violence and requires Member States to criminalise forms of cyber violence, including the non-consensual sharing of intimate or manipulated material, cyber stalking and cyber harassment.[39] These measures contribute to broader gender equality

[33] *Id.* § 67B.
[34] BNS, *supra* note 12, § 78(1)(ii).
[35] *Id.* § 356(1).
[36] *Id.* § 351(1), (4).
[37] IT Rules, *supra* note 29, rr. 2(1)(wa), 3(3); MINISTRY OF ELEC. & INFO. TECH., *Frequently Asked Questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026* (Feb. 10, 2026) (India).
[38] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, O.J. L, 2024/1689 (July 12, 2024), https://eur-lex.europa.eu/eli/reg/2024/1689/oj.
[39] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence, arts. 2(a), 5–8, O.J. L, 2024/1385 (May 24, 2024), https://eur-lex.europa.eu/eli/dir/2024/1385/oj; *see also* Press Release, European Commission, Commission Welcomes Political Agreement on New Rules to Combat Violence Against Women and Domestic Violence (Feb. 6, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_649 (last visited Nov. 22, 2026).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

initiatives[40] but should be integrated with AI-specific regulation to address abuses stemming directly from AI applications.

In response to emerging challenges, international standards urge technology companies to uphold human rights. At a recent virtual summit on deepfake abuse, civil society organisations discussed the need for an agreed definition of deepfakes and approaches to managing such content, including treating deepfakes as a violation of consent and requiring developers to remove deepfake content from their training data.[41] Search engines and AI developers could further help by limiting access to, and the distribution of, harmful content.

The Global Network Initiative, a coalition of civil society organisations and technology companies, encourages companies to respect freedom of expression and adhere to internationally recognised human rights standards, including the International Covenant on Civil and Political Rights (ICCPR). These protections alone are insufficient to combat gendered online violence. The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) should be enforced alongside the ICCPR to provide a more comprehensive defence of women's rights. Protection for whistleblowers in the technology sector is also essential to address digital violence and ensure the accountability of large technology corporations.[42]

Building "AI resilience" into online platforms is critical, and proactive measures, such as safety by design, are essential to mitigate gender-based violence online. PEN America has proposed measures that social media platforms can take to reduce online abuse while preserving free expression.[43] Civil society organisations also recommend labelling deepfake content and conducting rigorous testing (red-teaming) before products are launched. Reporters Without Borders calls for information professionals to supervise large language models during their training phase, so that outputs are reliable and ethical. Human reviewers who assess model outputs for accuracy, toxicity and other risk factors add another layer of mitigation.[44]

---

[40] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Union of Equality: Gender Equality Strategy 2020–2025*, COM (2020) 152 final (Mar. 5, 2020), https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/gender-equality/gender-equality-strategy_en (last visited Nov. 22, 2026).

[41] De Silva de Alwis & Vialle, *supra* note 7; *see also* James Vincent, *Why We Need a Better Definition of 'Deepfake'*, VERGE (May 22, 2018), https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news (last visited Nov. 22, 2026).

[42] De Silva de Alwis & Vialle, *supra* note 7.

[43] PEN AM., *No Excuse for Abuse: What Social Media Companies Can Do Now to Combat Online Harassment and Empower Users* (Mar. 2021), https://pen.org/report/no-excuse-for-abuse/; *see also* PEN AM., *Online Abuse Defense Training Program*, https://pen.org/program/online-abuse-defense-training-program/.

[44] De Silva de Alwis & Vialle, *supra* note 7.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

There is also a pressing need for effective escalation procedures for journalists and human rights defenders facing online threats. Because of staff turnover within technology companies, informal escalation channels, which rely on personal connections, are often unreliable. Civil society groups supporting women's rights advocate structured, responsive channels for urgent cases, and many of them have petitioned the UN for such reforms.[45]

For women journalists, digital literacy and resilience are priorities. Initiatives such as the Digital Dada Podcast in Kenya and East Africa raise awareness of digital literacy and gender-based violence. Expanding similar training worldwide could equip journalists with the skills to detect and prevent deepfake exploitation. Techniques such as adding noise to images or using filters that make slight edits can make deepfakes harder to create. Policymakers must recognise the connections between anti-feminism, threats to democracy and digital authoritarianism, and future legal reforms should consider the convergence of these risks to ensure that AI's role in society aligns with ethical and democratic values.[46]

V. Conclusion

The fight against cybercrimes targeting women is both essential and complex, demanding a multifaceted approach that addresses both legal and societal challenges. Addressing these crimes requires a robust legal system that not only adapts to technological change but also aligns with international standards set under CEDAW, by the United Nations and by the European Union. Strengthening national laws to reflect global standards will create a framework that both deters cybercrimes and upholds the fundamental rights of women in digital spaces.

Societal attitudes towards women's presence online must shift to recognise and respect fully women's right to bodily autonomy, personal integrity and privacy. Online violence against women, often a reflection of deeply ingrained gender biases and stereotypes, needs to be understood as part of a broader context of gender discrimination and power imbalances. Women's participation in online spaces should be encouraged without fear of harassment or objectification, promoting a more inclusive digital environment.

Empowering women to take proactive steps against online harassment is crucial. Features such as community guidelines, blocking and reporting mechanisms on social media platforms can help women address and mitigate cyber harassment. Women should not, however, be left to confront these challenges alone. Governments, law enforcement agencies and technology companies have a responsibility to provide resources, tools and training that enable effective

[45] *Id.*
[46] *Id.*

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

responses to cybercrimes. Enforcement agencies in particular must keep pace with technological advances, as offenders increasingly exploit gaps in knowledge and enforcement. Regular training for the police and other authorities on cybercrime trends will help close these gaps and improve the response to digital violence.

As AI and digital technologies become deeply embedded in daily life, it is essential to address the intersection between gender and technology. Policymakers must consider how AI technologies may disproportionately affect women, particularly in authoritarian regimes where AI-powered surveillance can target them for acts as simple as non-compliance with dress codes. Global AI governance frameworks should therefore prioritise ethical standards that protect women's rights, combating both gender-based violence and the misuse of technology to perpetuate discrimination. Only through a combination of strengthened laws, societal change and technological safeguards can a safer, more equitable digital world be created for all.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]