The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

CYBER GENDER VIOLENCE AND CONSTITUTIONAL MORALITY: A LEGAL ANALYSIS OF ONLINE HARMS AGAINST WOMEN

***TARANBIR SINGH**

ABSTRACT

In addition to redefining social interaction, communication, and information access, the digital revolution has also given rise to a new frontier of gendered violence. The rise of cyber gender violence, which includes online defamation, trolling, image-based sexual abuse, and cyberstalking, illustrates how patriarchal oppression has spread online. The internet, which was once thought of as an emancipatory space, now perpetuates structural injustices that jeopardise women's autonomy, privacy, and dignity. Such harms violate the rights to equality under Article 14, non-discrimination under Article 15(3), and life and personal liberty under Article 21 of the Indian Constitution. Both state and non-state actors must uphold the moral principles of equality, fraternity, and individual dignity enshrined in the Constitution, according to the theory of constitutional morality as expressed in progressive jurisprudence.[1]

Through the prism of constitutional morality, this study conducts a doctrinal and analytical investigation of cyber gender violence. It assesses the effectiveness of Indian legal tools, such as the Information Technology Act of 2000 and the Bharatiya Nyaya Sanhita of 2023, and looks at how digital victimisation and online harassment violate fundamental rights. Additionally, it makes use of comparative analysis from international agreements like the Budapest Convention on Cybercrime and the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). The study makes the case for a constitutionalised approach to cyber

[1] *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1, ¶¶ 116–120 (India).

jurisprudence, which sees online harms as breaches of the constitutional promise of dignity rather than just statutory violations.[2]

In the end, the study argues that the structural failure to translate constitutional values into the digital sphere is what constitutes cyber gender violence. In order to address this, India's cyber law system needs to develop into a framework based on constitutional morality, making sure that human dignity and gender justice are not subordinated to technological advancement.[3]

CHAPTER-I INTRODUCTION: THE DIGITAL TURN IN GENDER JUSTICE

A. THE EMERGENCE OF CYBER GENDER VIOLENCE IN THE AGE OF DIGITAL CITIZENSHIP

Technology's pervasiveness in daily life has changed how people interact with one another, participate in politics, and create identities. However, advancements in digital technology have also led to new forms of discrimination and control, which disproportionately impact women. Traditional patriarchal harms in virtual spaces have been reconstituted by behaviours like doxxing, morphing, cyberstalking, and the unconsented sharing of intimate images.[4] Cyberspace's anonymity gives offenders more confidence while making redress difficult, particularly in countries where gender bias and the digital literacy gap still exist.

Therefore, cyber gender violence is a manifestation of systemic gender inequality rather than a technological anomaly. It has been described by academics as a "continuum of violence" that cuts across time and space, connecting digital abuse to offline subordination.[5] Social media's growth has further dissolved the lines between public and private life, making women's expression, appearance, and political participation vulnerable to criticism and hostility. Online harassment is acknowledged by the UN Human Rights Council as a type of gender-based violence, and states are urged to take appropriate measures to stop and address these violations.[6]

---

[2] Convention on the Elimination of All Forms of Discrimination Against Women art. 1, Dec. 18, 1979, 1249 U.N.T.S. 13; Council of Europe, *Convention on Cybercrime* (Budapest Convention), Nov. 23, 2001, E.T.S. No. 185.

[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶¶ 297–302 (India); *Joseph Shine v. Union of India*, (2019) 3 S.C.C. 39, ¶¶ 124–130 (India).

[4] National Crime Records Bureau, *Crime in India: 2021 Statistics*, Ministry of Home Affairs, Gov't of India (2022).

[5] Jac sm Kee, *Feminist Principles of the Internet* 4 (Association for Progressive Communications, 2016).

[6] U.N. Hum. Rts. Council, *Report of the Special Rapporteur on Violence Against Women, Its Causes and Consequences*, U.N. Doc. A/HRC/38/47, ¶¶ 31–33 (2018).

B. RESEARCH OBJECTIVES, HYPOTHESIS, AND METHODOLOGY

The premise of this paper is that cyber-gender violence violates the Indian Constitution's fundamental rights and morals. The main goals are:

1. To investigate the constitutional and theoretical foundations of cyber-gender violence;
2. to evaluate whether Indian statutory responses, particularly the Bharatiya Nyaya Sanhita, 2023, and the Information Technology Act, 2000, are adequate;
3. To examine how digital gender harms are governed by international law; and
4. To put forth a gender-sensitive, normative model of cyber governance that is based on constitutional morality.

Using primary legal sources, statutory interpretation, judicial precedents, and comparative international materials, the methodology is doctrinal and analytical. The study takes a constitutional hermeneutic stance, purposefully interpreting fundamental rights to conform to changing digital realities.[7] The empirical background of this work is informed by studies conducted by the United Nations Office on Drugs and Crime (UNODC) and reports from the National Crime Records Bureau (NCRB).[8]

C. SIGNIFICANCE OF THE STUDY WITHIN THE INDIAN CONSTITUTIONAL FRAMEWORK

This study is important because it reframes cyber gender violence as a constitutional wrong rather than just a criminal offence. The Supreme Court of India has upheld the concept of constitutional morality, which requires state institutions to respect the moral precepts of equality, liberty, and fraternity.[9] The constitutional guarantees of dignity under Article 21 and equality under Articles 14 and 15 are directly violated when acts of digital harassment, online defamation, and image-based abuse are viewed through this lens.[10]

Protecting women's online spaces becomes a constitutional requirement in a time when having a digital presence is a crucial aspect of citizenship. The state's obligation to defend citizens against state and non-state interference is emphasised by the Supreme Court's Puttaswamy ruling, which recognised the right to privacy as essential to individual liberty.[11] The judiciary's readiness to adapt gender jurisprudence in response to novel forms of harm is also

[7] *Maneka Gandhi v. Union of India*, (1978) 1 S.C.C. 248, ¶ 56 (India).
[8] United Nations Office on Drugs & Crime, *The Global Report on Cybercrime and Gender-Based Violence* (2021).
[9] *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1, ¶¶ 118–121 (India).
[10] *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 S.C.C. 608, ¶¶ 6–8 (India).
[11] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶¶ 297–302 (India).

demonstrated by the landmark rulings in Vishaka v. State of Rajasthan and Laxmi v. Union of India.[12] Therefore, applying this jurisprudence to cyberspace is not just sensible; it is necessary to fulfil the substantive equality guarantee of the Constitution.

CHAPTER-II CONCEPTUALISING CYBER GENDER VIOLENCE: A JURISPRUDENTIAL PERSPECTIVE

A. UNDERSTANDING CYBER GENDER VIOLENCE: BEYOND CONVENTIONAL NOTIONS OF CRIME

Cyber gender violence is more than just cybercrime. Any act that causes or threatens to cause physical, sexual, psychological, or financial harm to women and gender minorities in cyberspace is considered a gendered form of violence enabled by digital technologies.[13] In contrast to traditional crimes, cyber violence occurs in an anonymous, borderless setting where offenders use digital tools to increase surveillance, intimidation, and patriarchal control.

Academics contend that cyber gender violence needs to be understood as a continuum of structural subordination ingrained in social hierarchies rather than just as aberrant online conduct.[14] As patriarchal ideology adjusts to digital infrastructures, the virtual world replicates the systemic disparities of the real one. Thus, rather than being isolated crimes, online harassment, sexual extortion, and digital shaming become manifestations of gender power dynamics. This phenomenon is acknowledged as a "global pandemic of online abuse" by the United Nations Broadband Commission for Sustainable Development, which calls on governments to implement gender-responsive cyber policies.[15]

The lack of a statutory definition of "cyber gender violence" in Indian law has led to interpretive difficulties. Without taking into account the gendered nature of harm, the majority of cases are prosecuted under general provisions of the Bharatiya Nyaya Sanhita, 2023, or the Information Technology Act, 2000. This legal gap emphasises how important it is to create a unique body of law on digital gender justice that incorporates feminist, constitutional, and criminological ideas.[16]

---

[12] *Vishaka v. State of Rajasthan*, (1997) 6 S.C.C. 241, ¶ 16 (India); *Laxmi v. Union of India*, W.P. (Crl.) No. 129 of 2006, ¶ 13 (S.C. Apr. 10, 2015) (India).
[13] U.N. Women, *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call* 2–3 (2015).
[14] Catherine MacKinnon, *Toward a Feminist Theory of the State* 238–45 (Harvard Univ. Press 1989).
[15] U.N. Broadband Comm'n for Sustainable Dev., *Cyber Violence Against Women and Girls: A Global Report* 4–5 (2015).
[16] Pavan Duggal, *Cyberlaw: The Indian Perspective* 203–05 (2d ed. 2021).

B. THE CONTINUUM OF OFFLINE PATRIARCHY AND ONLINE HARMS

It is neither new nor coincidental that patriarchal practices have moved online. The internet is not a neutral space; rather, it reflects existing power imbalances, according to feminist legal theorists.[17] Social media's anonymity and amplification tools support discriminatory stereotypes, and algorithmic biases support misogynistic narratives. Once thought of as platforms for emancipation, online spaces frequently turn into theatres of dominance where women's identities, voices, and bodies are scrutinised and turned into commodities.

Digital voyeurism, revenge pornography, and targeted hate campaigns are examples of phenomena that demonstrate this continuum between offline and online oppression. By restricting women's ability to participate in public discourse, each act perpetuates gender hierarchies.[18] The psychological distress and harm to one's reputation that arise from such abuse are similar to, and frequently worse than, the harm that occurs in physical environments. Therefore, it is necessary to conceptualise cyber gender violence as a component of the broader feminist fight for communicative freedom and bodily autonomy, which is based on constitutional guarantees of equality and dignity.[19]

C. TYPOLOGY OF ONLINE VIOLENCE AGAINST WOMEN

Although cyberviolence takes many forms as technology advances, some trends have been recognised by the legal and social sciences. These consist of:

1. Cyberstalking and Online Surveillance: Constant monitoring, communication, or harassment via digital media with the intention of causing fear or control is known as cyberstalking and online surveillance. It is illegal under §78 of the Bharatiya Nyaya Sanhita, 2023, and it infringes on the privacy and personal liberty guaranteed by Article 21 of the Constitution.[20]
2. Image-Based Sexual Abuse (IBSA): A serious violation of the right to dignity is committed when intimate images, such as deepfakes and revenge pornography, are created or distributed without consent. Articles 66E, 67, and 67A of the Information Technology Act of 2000 apply to such acts.[21]

---

[17] Anita Gurumurthy & Nandini Chami, *Gender Equality in the Digital Age: A Feminist Framework for Policy and Law* 6–8 (IT for Change, 2016).
[18] Danielle Citron, *Hate Crimes in Cyberspace* 24–29 (Harvard Univ. Press 2014).
[19] Flavia Agnes, *Gender, Law and the Constitution: A Feminist Re-reading of Indian Jurisprudence*, 13 **Nat'l L. Sch. India Rev.** 1, 12–14 (2001).
[20] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 78 (India).
[21] Information Technology Act, No. 21 of 2000, §§ 66E, 67 & 67A (India).

3. Doxxing and Identity Theft: According to §§66C and 66D of the Information Technology Act, doxxing and identity theft are defined as the willful posting of personal information or impersonation online that results in targeted threats or defamation.[22]
4. Trolling and Online Hate Speech: Online hate speech and trolling are coordinated efforts to silence women's voices through sexualized abuse. Although such speech is implicated in Article 19(1)(a), courts have recognised that it may be restricted under Article 19(2) in order to preserve decency and public order.[23]
5. Sextortion and Online Blackmail: Online blackmail and sextortion are the coercive use of digital content to obtain money or sexual favours; they are frequently prosecuted under related cyber provisions or §§383–389 of the Bharatiya Nyaya Sanhita.[24]

These categories, which combine psychological coercion, reputational harm, and constitutional rights violations, each highlight the multifaceted nature of cyber gender violence.

D. PSYCHOLOGICAL AND VICTIMOLOGICAL DIMENSIONS OF DIGITAL HARMS

Cyber gender violence has serious psychological and victimological repercussions that go beyond the legal perspective. According to studies, the ongoing and pervasive nature of digital abuse causes survivors to suffer from anxiety, depression, and post-traumatic stress disorder.[25] Feelings of social isolation and vulnerability are made worse by losing control over one's online identity. The World Health Organisation acknowledges that the decline in mental health brought on by cyberbullying is a real public health issue.[26]

From a victimological perspective, vulnerability is exacerbated by the intersection of digital literacy, gender, and class. The lack of access to redressal mechanisms exacerbates the harm experienced by marginalised women, especially those from minority, Dalit, or rural communities.[27] International law recognises the state's duty of due diligence, which calls for preventive and corrective actions, such as psychological support and easily accessible grievance procedures.[28] The state is required by the Indian Constitution to establish conditions

[22] Id. §§ 66C–66D.
[23] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 82–87 (India).
[24] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 383–389 (India).
[25] Amnesty Int'l, *Troll Patrol India: Exposing Online Abuse Faced by Women Politicians in India* 11–13 (2021).
[26] World Health Org., *Mental Health and Digital Environments: Global Report* 18–20 (2022).
[27] Ranjana Kumari, *Cyber Violence and Marginalised Women: India's Hidden Crisis*, **Centre for Social Research Report** 9–10 (2020).
[28] U.N. Hum. Rts. Council, *Due Diligence Framework on Violence Against Women*, U.N. Doc. A/HRC/23/49, ¶¶ 13–17 (2013).

that guarantee women's equal participation in digital life, as stated in Articles 38 and 39 of the Directive Principles.[29]

CHAPTER-IV CONSTITUTIONAL MORALITY AND THE DIGITAL SPHERE

A. THE DOCTRINE OF CONSTITUTIONAL MORALITY: CONCEPT AND EVOLUTION

The idea of constitutional morality embodies the normative core of the Indian Constitution, serving as an ethical compass that directs state and private behaviour in line with the principles of equality, liberty, and fraternity. Although the term was initially used in the debates of the Constituent Assembly, the Supreme Court gave it jurisprudential depth in a number of significant cases.[30] Constitutional morality, according to Dr. B.R. Ambedkar, is a principle that ensures that governance conforms to constitutional ethos rather than social or religious orthodoxy and restrains majoritarian impulses.[31]

The Court upheld that constitutional morality necessitates "institutional respect, accountability, and adherence to the democratic spirit" in the case of Government of the NCT of Delhi v. Union of India.[32] Justice Chandrachud went on to explain in Navtej Singh Johar v. Union of India that constitutional morality embodies the fundamental commitment to human dignity and that the state must eliminate social hierarchies that obstruct individual autonomy.[33] The state's duty to uphold rights in both real and virtual spaces has been shaped by this interpretive development, which has turned constitutional morality from a philosophical ideal into a legally binding principle.

When it comes to cyberspace, constitutional morality requires that digital governance and technology regulation align with the moral principles of the Constitution. Constitutional morality serves as the normative check that keeps the virtual public sphere democratic, inclusive, and dignified in a time when private platforms have near-sovereign control over speech, privacy, and identity.[34]

---

[29] INDIA CONST. arts. 38 & 39.
[30] *Gov't of NCT of Delhi v. Union of India*, (2018) 8 S.C.C. 501, ¶ 193 (India).
[31] Constituent Assembly Debates, Vol. VII, 38 (Nov. 4, 1948) (statement of Dr. B.R. Ambedkar).
[32] *Gov't of NCT of Delhi v. Union of India*, (2018) 8 S.C.C. 501, ¶ 193 (India).
[33] *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1, ¶¶ 116–120 (India).
[34] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* 225–27 (HarperCollins 2019).

B. GENDER EQUALITY AS A FACET OF CONSTITUTIONAL MORALITY

An essential part of constitutional morality is gender justice. Gender equality was purposefully incorporated into the Constitution's substantive and structural provisions by its framers; Articles 14 and 15(3) guarantee equal protection and give the state the authority to implement affirmative action policies for women.[35] In *Air India v. Nergesh Meerza*, the court acknowledged that equality is a dynamic concept that needs contextual interpretation rather than being a sterile abstraction.[36]

The Supreme Court ruled in *Anuj Garg v. Hotel Association of India* that gender-based limitations with paternalistic roots go against the spirit of constitutional morality.[37] This principle forces the legislature and judiciary to consider the morality of state action in gendered contexts in addition to its legality. Therefore, cyber gender violence is a violation of the Constitution because its acceptance or lack of regulation threatens the moral foundation of equality that upholds the Republic.

The state is positively obligated by constitutional morality to guarantee substantive gender justice in digital spaces, given the prevalence of algorithmic biases, data surveillance, and online misogyny in the digital age.[38] In order to safeguard women from state and private digital actors who jeopardise their participation and dignity, the constitutional guarantee of equality must be expanded technologically.

C. JUDICIAL EXPANSION OF ARTICLES 14, 15(3), 19, AND 21 IN THE CONTEXT OF DIGITAL RIGHTS

The judicial extension of constitutional guarantees into the digital sphere has been a defining feature of India's evolving fundamental rights jurisprudence. Digital discrimination and algorithmic injustice are now covered by Article 14, which upholds the right to equality before the law.[39] Affirmative action is permitted under Article 15(3) to protect women, which naturally includes protecting them from harms that may arise online.

Although freedom of speech and expression is guaranteed by Article 19, the conflict between liberty and harm has been made clear by digital speech. The Court ruled in Shreya Singhal v.

---

[35] INDIA CONST. arts. 14 & 15(3).
[36] *Air India v. Nergesh Meerza*, (1981) 4 S.C.C. 335, ¶¶ 38–41 (India).
[37] *Anuj Garg v. Hotel Ass'n of India*, (2008) 3 S.C.C. 1, ¶¶ 44–46 (India).
[38] U.N. Gen. Assembly, *Resolution on the Promotion of Women's Equal Access to Information and Communication Technologies*, A/RES/68/181 (Dec. 18, 2013).
[39] Abhinav Chandrachud, *Equality in the Digital Age: Algorithmic Bias and the Constitution of India*, 63 **J. Indian L. Inst.** 245, 248–49 (2021).

Union of India that ambiguous limitations on online speech are in violation of Article 19(1)(a) and invalidated §66A of the Information Technology Act, 2000.[40] But the Court also underlined that, in accordance with Article 19(2), freedom of expression is not unqualified and must give way when it incites hatred or jeopardises dignity. The constitutional foundation for controlling online hate speech and gendered abuse is this balance.

Most significantly, the rights to privacy, reputation, and mental integrity have been incorporated into Article 21—the right to life and personal liberty. The Supreme Court ruled in *Justice K.S. Puttaswamy (Retd.) v. Union of India* that the "right to control dissemination of personal information" is a component of privacy.[41] Article 21 is directly violated when women are stalked online or when private photos are shared without permission. In a similar vein, the Court expanded Article 21 obligations to include non-state actors whose actions or words compromise dignity in *Kaushal Kishor v. State of Uttar Pradesh*.[42] When taken as a whole, these cases establish cyber gender violence as a fundamental rights violation rather than just a legal infraction.

D. CYBER HARMS AS CONSTITUTIONAL WRONGS: PRIVACY, DIGNITY, AND AUTONOMY IN THE ONLINE DOMAIN

The moral universe of the Constitution aims for a comprehensive understanding of personhood in which autonomy, privacy, and dignity are intertwined.[43] The core of these rights is undermined by cyber harms, whether they take the shape of online harassment, digital stalking, or abuse based on images. By fostering a climate of fear and silence, such actions not only harm women's reputations but also undermine their constitutional agency.

The Supreme Court acknowledged in R. Rajagopal v. State of Tamil Nadu that an individual's control over their personal information and public image is protected by their right to privacy.[44] Digital application of this principle results in constitutional violations for doxxing and non-consensual image sharing. According to Francis Coralie Mullin v. Administrator, Union Territory of Delhi, the right to dignity encompasses not only physical integrity but also mental and reputational well-being.[45] Therefore, it is against constitutional morality to harass women online in a way that diminishes their personhood.

---

[40] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 82–87 (India).
[41] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶¶ 297–302 (India).
[42] *Kaushal Kishor v. State of Uttar Pradesh*, (2023) 2 S.C.C. 1, ¶¶ 158–160 (India).
[43] *Joseph Shine v. Union of India*, (2019) 3 S.C.C. 39, ¶ 124 (India).
[44] *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 S.C.C. 632, ¶ 26 (India).
[45] *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 S.C.C. 608, ¶¶ 6–8 (India).

Therefore, the constitutional response to cyber harms must move beyond punitive law and toward restorative digital justice, giving survivors' dignity, rehabilitation, and systemic accountability top priority.[46] In this way, constitutional morality serves as the moral code of the digital state, a concept that turns the internet into a place of rights rather than dominance.

CHAPTER-V LEGAL ARCHITECTURE IN INDIA: STATUTORY AND JUDICIAL RESPONSE

A. CONSTITUTIONAL SAFEGUARDS AND FUNDAMENTAL RIGHTS OF WOMEN IN CYBERSPACE

With its guarantees of equality, dignity, and liberty, the Indian constitutional framework offers a strong normative basis for safeguarding women against cyber harms. Together, Articles 14, 15, 19, and 21 establish a constitutional umbrella that encompasses the digital sphere.[47] The Constitution is a living document that can adapt to changing social realities and technological advancements, as the Supreme Court has underlined time and time again.[48]

All state and non-state actors are required by Article 14 to respect the principle of non-arbitrariness, which includes treating women equally in digital settings. Affirmative action by the state to protect women's rights is permitted by Article 15(3), which gives legitimacy to gender-specific cyber laws and remedial frameworks.[49] Additionally, the right to privacy, reputation, and mental health, all of which are linked to online harassment and image-based abuse, have been judicially extended to include the guarantee of life and personal liberty in Article 21.[50]

A constitutional dialectic between the right to dignity and freedom of expression has resulted from the intersection of Articles 19(1)(a) and 21. Online speech is protected by Article 19(1)(a), but restrictions based on morality and decency are permitted by Article 19(2). These clauses need to be reconciled in light of gendered cyber abuse using a constitutional morality framework to maintain the freedom and security of the online public sphere.[51]

---

[46] U.N. Hum. Rts. Council, *Guidelines on Gender Justice and Digital Rights*, U.N. Doc. A/HRC/46/49, ¶¶ 22–27 (2021).
[47] INDIA CONST. arts. 14, 15, 19 & 21.
[48] *People's Union for Civil Liberties v. Union of India*, (1997) 1 S.C.C. 301, ¶ 18 (India).
[49] *Charu Khurana v. Union of India*, (2015) 1 S.C.C. 192, ¶¶ 38–40 (India).
[50] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶¶ 297–302 (India).
[51] *Subramanian Swamy v. Union of India*, (2016) 7 S.C.C. 221, ¶¶ 88–90 (India).

B. THE INFORMATION TECHNOLOGY ACT, 2000: SCOPE, GAPS, AND JUDICIAL INTERPRETATION

India's first comprehensive law addressing data protection, cybercrimes, and electronic communication was the Information Technology Act, 2000 (IT Act). It was first created to support digital authentication and e-commerce, but its purview was later extended to include cybercrime. Identity theft, impersonation, and the publication or transmission of pornographic material in electronic form are all prohibited by Sections 66C to 67B.[52] The provisions 67 (obscene material), 67A (sexually explicit content), and §§66E (violation of privacy) that penalise the non-consensual dissemination of intimate imagery and voyeurism are particularly pertinent to gendered harms. [53]

Nevertheless, the IT Act has a number of structural and legal flaws. First of all, because gendered cyber violence is not explicitly acknowledged, gender-neutral enforcement ignores the disproportionate harm done to women. Second, there are jurisdictional conflicts and procedural ambiguity due to its provisions overlapping with the Bharatiya Nyaya Sanhita, 2023. Third, enforcement organisations frequently depend on arbitrary definitions of "obscenity," which compromises women's freedom of expression online.[54]

These gaps have been somewhat filled by judicial interpretation. The Supreme Court ruled in Shreya Singhal v. Union of India that §66A of the IT Act was unconstitutional because it violated Article 19(1)(a) by imposing ambiguous restrictions on online speech.[55] This ruling highlighted the need for specific legal tools to combat online abuse without infringing on civil liberties, even as it upheld the importance of free speech. Similar to this, the Court reinterpreted "obscenity" in Aveek Sarkar v. State of West Bengal in a contemporary, contextual way, stating that representations of sexuality are protected unless they tend to be corrupt or deprave.[56] Together, these decisions highlight the court's efforts to strike a balance between freedom and dignity in the online sphere.

C. THE BHARATIYA NYAYA SANHITA, 2023: A CONTEMPORARY PENAL RESPONSE TO DIGITAL HARMS

A number of provisions pertaining to digital crime have been modernised by the Bharatiya Nyaya Sanhita, 2023 (BNS), which has replaced the Indian Penal Code. It specifically

[52] Information Technology Act, No. 21 of 2000, §§ 66C–67B (India).
[53] Id. §§ 66E, 67, 67A.
[54] Sahana Basavapatna, *Gendered Dimensions of Cyber Law in India*, **Indian J. Criminology**, Vol. 47, No. 2, at 15–18 (2019).
[55] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 82–87 (India).
[56] *Aveek Sarkar v. State of West Bengal*, (2014) 4 S.C.C. 257, ¶¶ 18–20 (India).

acknowledges crimes such as voyeurism, cyberstalking, and the distribution of images without consent. While stalking via any electronic means is illegal under Section 78, voyeurism, which includes recording or disclosing private acts without permission, is punishable under Section 77.[57]

Despite being a sign of legislative progress, these provisions remain reactive and punitive in nature, rather than preventive or rehabilitative. Their effectiveness is limited by the lack of precise guidelines for intermediary liability, data protection, and consent. Furthermore, there is still a lack of coordination between the BNS, the IT Act, and the Digital Personal Data Protection Act of 2023.[58] As a result, India still lacks a cohesive legal framework that addresses cyber gender violence as a separate category of harm based on constitutional rights, even after the BNS was modernised.

D. JUDICIAL INTERVENTIONS AND LANDMARK CASES: FROM *RITU KOHLI* TO *SHREYA SINGHAL*

In the landmark case of *Ritu Kohli v. State (NCT of Delhi),* the Delhi Police filed India's first cyberstalking case under §509 of the Indian Penal Code and §67 of the IT Act, establishing the country's legal precedent on cyber gender violence.[59] This case demonstrated how inadequate the current legal framework is to handle invasions of privacy in digital spaces.

One of the first convictions under §67 of the IT Act was in *State of Tamil Nadu v. Suhas Katti*, where the accused was found guilty of posting offensive messages and disparaging remarks about a woman in a Yahoo chat group.[60] Although its success was an anomaly, the case showed the potential of digital evidence in cybercrime prosecutions.

The 2015 Shreya Singhal decision by the Supreme Court marks a turning point in constitutional history. The Court protected online speech by declaring §66A unconstitutional, but it also made clear that states must create laws specifically designed to address real harms, such as online harassment.[61] Similar to this, the Court established judicial precedent for platform accountability in *Sabu Mathew George v. Union of India* by ordering intermediaries like Google and Facebook to block ads pertaining to prenatal sex determination.[62] All of these rulings support the idea that digital responsibility and freedom are inextricably linked.

---

[57] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 77–78 (India).
[58] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[59] *Ritu Kohli v. State (NCT of Delhi)*, 2001 Cri. L.J. 212 (Del.) (India).
[60] *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004 (C.J.M. Ct., Egmore, 2004) (India).
[61] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 82–87 (India).
[62] *Sabu Mathew George v. Union of India*, (2018) 3 S.C.C. 229, ¶¶ 12–14 (India).

E. ENFORCEMENT CHALLENGES: INVESTIGATIVE LIMITATIONS AND PROCEDURAL BARRIERS

Even with an expanding body of legislation, there are still many institutional and procedural flaws in the way cyber laws are enforced. Cybercrime is increasing annually, according to the National Crime Records Bureau (NCRB), but conviction rates are still disproportionately low.[63] The absence of cyber-forensic infrastructure, jurisdictional ambiguity in transnational offences, and a lack of gender-sensitisation among law enforcement officials are some of the factors that contribute to this disparity.

Furthermore, the Ministry of Home Affairs' online complaint portals and other grievance redressal mechanisms are disjointed and underutilised.[64] Due to insensitive police practices, social stigma, and a lack of digital literacy, survivors frequently experience secondary victimisation. The state is required by the principle of due diligence, which is acknowledged by both international law and domestic constitutional jurisprudence, to effectively prevent, investigate, and remedy such harms.[65] The promise of constitutional protection in cyberspace runs the risk of remaining illusory in the absence of victim-centric mechanisms and institutional reform.

CHAPTER-VI INTERNATIONAL AND COMPARATIVE LEGAL FRAMEWORKS

A. INTERNATIONAL INSTRUMENTS: CEDAW, ICCPR, ICESCR, AND THE BUDAPEST CONVENTION

Because cyber gender violence crosses national boundaries, an international legal response based on universal human rights principles is required. The cornerstone of the international normative framework for gender equality is still the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), which India ratified in 1993.[66] Through the principle of evolving interpretation, CEDAW's obligations extend to the online realm even though it was adopted before the digital age. General Recommendation No. 35 of the CEDAW

[63] National Crime Records Bureau, *Crime in India 2022: Statistics*, Ministry of Home Affairs, Gov't of India, at 514–516 (2023).
[64] Ministry of Home Affairs, *National Cyber Crime Reporting Portal – Annual Report* (2023).
[65] U.N. Hum. Rts. Council, *Due Diligence Framework on Violence Against Women*, U.N. Doc. A/HRC/23/49, ¶¶ 13–17 (2013).
[66] Convention on the Elimination of All Forms of Discrimination Against Women, Dec. 18, 1979, 1249 U.N.T.S. 13.

Committee requires states to prevent, investigate, and punish gender-based violence in digital contexts.[67]

Likewise, Articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR) guarantee the freedom of expression, privacy, and dignity, all of which are equally applicable in cyberspace.[68] While General Comment No. 16 affirms the state's obligation to protect individuals against privacy intrusions by both public and private actors, General Comment No. 34 of the Human Rights Committee states that limitations on digital expression must be legal, necessary, and proportionate.[69]

Common criminal standards for cyber offences, such as unauthorised access, data interference, and content-based crimes, are established by the 2001 Budapest Convention on Cybercrime, the first international agreement addressing offences related to computers and the internet.[70] India is not a signatory, but its tenets have influenced domestic jurisprudence and the harmonisation of cyber law worldwide. The framework is further expanded by the Council of Europe's Convention on Preventing and Combating Violence Against Women and Domestic Violence (Istanbul Convention), which specifically addresses technology-facilitated abuse as a violation of women's human rights.[71]

These tools collectively impose a triadic duty on states: to prevent cyber gender violence through education and legislation, to protect victims through enforcement and remedies, and to prosecute offenders through international cooperation and due diligence.[72]

B. REGIONAL DEVELOPMENTS: THE GDPR AND THE EUROPEAN HUMAN RIGHTS MODEL

A landmark piece of international privacy law is the General Data Protection Regulation (GDPR) of the European Union, which views data protection as an extension of human autonomy and dignity.[73] Lawfulness, fairness, and accountability are outlined in Articles 5 and

---

[67] Comm. on the Elimination of Discrimination Against Women, *General Recommendation No. 35 on Gender-Based Violence Against Women Updating General Recommendation No. 19*, U.N. Doc. CEDAW/C/GC/35, ¶¶ 20–22 (July 26, 2017).
[68] International Covenant on Civil and Political Rights arts. 17 & 19, Dec. 16, 1966, 999 U.N.T.S. 171.
[69] Hum. Rts. Comm., *General Comment No. 16: Article 17 (Right to Privacy)*, U.N. Doc. HRI/GEN/1/Rev.9
[70] Council of Eur., *Convention on Cybercrime (Budapest Convention)*, Nov. 23, 2001, E.T.S. No. 185.
[71] Council of Eur., *Convention on Preventing and Combating Violence Against Women and Domestic Violence (Istanbul Convention)*, May 11, 2011, C.E.T.S. No. 210.
[72] Rebecca MacKinnon, *Networked Authoritarianism and Human Rights in the Digital Age*, 24 **J. Democracy** 32, 34–35 (2013).
[73] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

6 of the GDPR, which also require express consent before collecting and using personal data. One significant protection against the ongoing spread of non-consensual intimate images—one of the most harmful types of cyber gender violence—is offered by the GDPR, which grants people the right to be forgotten under Article 17.[74]

At the same time, the European Court of Human Rights (ECHR) has construed digital privacy as being covered by Article 8 of the European Convention on Human Rights. The Court ruled in K.U. v. Finland that in order to protect a child's privacy and dignity, states have a positive duty to find and prosecute anonymous online offenders.[75] Thus, the jurisprudence of the ECHR upholds a fundamental moral principle of the constitution: the obligation of the state to take affirmative action to shield citizens from private harms in the digital realm.

A gender perspective is also incorporated into digital governance through European regional frameworks. Cyber violence is a continuum of gender-based violence, according to the European Institute for Gender Equality (EIGE), which emphasizes the need for digital regulation to be in line with equality mandates.[76] This all-encompassing strategy, which connects gender justice, data protection, and privacy, provides insightful guidance for India's developing cyber law system.

C. COMPARATIVE JURISPRUDENCE: LESSONS FROM THE UNITED STATES, UNITED KINGDOM, AND AUSTRALIA

Although the extent of legal responses to cyber gender violence has varied by jurisdiction, they all show a growing understanding that digital harms implicate human and constitutional rights.

Although there isn't a comprehensive federal cyber law in the US, several states have passed laws prohibiting online harassment, cyberstalking, and revenge pornography.[77] The historic People v. Bollaert case confirmed that non-consensual distribution of intimate images is prohibited in California and that the First Amendment does not protect such acts.[78] However, American jurisprudence still struggles to strike a balance between privacy and free speech in digital settings.

---

[74] Id. art. 17.
[75] *K.U. v. Finland*, App. No. 2872/02, ¶¶ 43–47 (Eur. Ct. H.R. Dec. 2, 2008).
[76] European Institute for Gender Equality, *Cyber Violence Against Women and Girls: A European Perspective* 6–7 (2017).
[77] Danielle Keats Citron & Mary Anne Franks, *Criminalising Revenge Porn*, 49 **Wake Forest L. Rev.** 345, 347–50 (2014).
[78] *People v. Bollaert*, 241 Cal. App. 4th 947, 955 (Cal. Ct. App. 2015).

The UK's legislative response has become more unified. Retaliation pornography is illegal under the Criminal Justice and Courts Act of 2015, and social media companies are required to take precautions to avoid harmful content under the Online Safety Act of 2023.[79] An emerging model of co-regulated digital governance that aligns with the participatory ideals of constitutional morality is the UK's approach, which places a strong emphasis on platform accountability and regulatory oversight.

The e-Safety Commissioner was created in Australia by the Enhancing Online Safety Act, 2015, and is a specialised authority with the authority to help victims and order the removal of non-consensual intimate material.[80] The importance of quick, victim-centred processes is emphasised by this model, which combines administrative redressal with criminal law. This lesson is especially pertinent given India's disjointed enforcement environment.

In contrast, these jurisdictions show that a multi-layered framework comprising platform obligations, criminal penalties, and survivor-centred remedies is necessary for effective cyber regulation. To varying degrees, each system operationalises the moral logic of constitutionalism, which holds that digital justice and individual dignity are inextricably linked.[81]

D. GLOBAL TRENDS TOWARDS GENDER-SENSITIVE CYBER GOVERNANCE

There is increasing international agreement that a gender-sensitive perspective needs to be incorporated into cyber governance. As "digital sovereigns," technology companies have human rights obligations comparable to those of state actors when it comes to policing online content, according to the United Nations Human Rights Council (2021).[82] The World Economic Forum and UNESCO advocate for digital literacy, algorithmic transparency, and inclusion of women in tech policy-making as essential components of cyber equality.[83]

These advancements suggest a new paradigm of digital constitutionalism in which transnational digital governance is guided by constitutional values such as equality, autonomy, and dignity. For India, a key player in the global digital ecosystem, bringing domestic laws into

[79] Criminal Justice and Courts Act 2015, c. 2, § 33 (U.K.); Online Safety Act 2023, c. 40 (U.K.).
[80] Enhancing Online Safety Act 2015 (Cth) § 7 (Austl.).
[81] Susan Benesch, *Defining and Deterring Hate Speech in the Digital Age*, 36 **Am. J. Comp. L.** 119, 122–23 (2018).
[82] U.N. Hum. Rts. Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/47/25, ¶¶ 48–52 (2021).
[83] UNESCO, *The Gender Dimensions of ICT Policy and Internet Governance* 9–11 (2022).

line with international norms is not just a matter of compliance but also of practical constitutional morality.[84]

CHAPTER-VII VICTIMOLOGICAL REALITIES AND SOCIO-LEGAL CHALLENGES

A. THE FEMINIST CEIMINOLOGY OF CYBER VIOLENCE

Digital victimisation is both structural and intersectional, according to victimological research on cyber gender violence. According to feminist criminology, this kind of violence is a continuation of patriarchal control, with technology serving as a new tool for oppression.[85] Despite its potential for emancipation, the internet perpetuates power imbalances that stigmatise, silence, and monitor women.

Digital victimisation is a systemic denial of agency that cannot be limited to the legal definitions of "obscenity" or "harassment." Victim vulnerability is increased by the permanence of digital records, the anonymity of offenders, and the spread of harmful content.[86] According to feminist legal scholars, the "cyber patriarchy" uses deepfakes, trolling, and memes to perpetuate gender hierarchies through networked abuse.[87] Such behaviour reflects the structural persistence of misogyny adapted to digital architecture and is not incidental; rather, it is ideological.

This violence goes right to the heart of Article 21's guarantee of mental integrity and dignity from a constitutional perspective. In addition to being administratively negligent, the state's failure to stop or address these harms is a constitutional omission.[88] Traditional criminal law frameworks have not yet met the substantive protection of women's digital personhood, which is a requirement of the constitutional promise of equality under Article 14.

B. PSYCHOLOGICAL TRAUMA AND THE RIGHT TO MENTAL HEALTH

The psychological harm caused by cyber gender violence is on par with the physical harm. Because digital abuse is so common and persistent, victims endure long-term anxiety, depression, PTSD, and social disengagement.[89] In contrast to traditional crimes, the online

---

[84] Gautam Bhatia, *Digital Constitutionalism and the Indian State*, **Indian L. Rev.**, Vol. 6, No. 2, at 189–92 (2022).
[85] Meda Chesney-Lind & Lisa Pasko, *The Female Offender: Girls, Women, and Crime* 112–14 (3d ed. 2013).
[86] Danielle Citron, *Hate Crimes in Cyberspace* 27–29 (Harvard Univ. Press 2014).
[87] Anita Gurumurthy & Nandini Chami, *Feminist Frameworks for Digital Rights: The Politics of Cyber Patriarchy*, **IT for Change Working Paper** 5–7 (2020).
[88] *Vishaka v. State of Rajasthan*, (1997) 6 S.C.C. 241, ¶¶ 16–17 (India).
[89] Amnesty Int'l, *Troll Patrol India: Exposing Online Abuse Faced by Women Politicians in India* 8–12 (2021).

setting permits re-victimisation on a regular basis; each comment, share, or repost feeds the trauma.

According to international human rights law, the World Health Organisation (WHO) acknowledges mental health as a crucial part of the right to health.[90] Psychological well-being has also been recognised by the Indian judiciary as a component of the right to life and dignity. The Supreme Court ruled in X v. Health and Family Welfare Department that mental health must be construed in a way that respects privacy and autonomy.[91] According to Article 21's constitutional definition of "life," the state is therefore required to protect women from psychological harm in both real-world and virtual contexts.

There is still very little access to mental health care, particularly in rural areas where victims frequently experience disbelief and exclusion. More than 70% of women who experience online abuse endure long-lasting psychological distress without access to formal counselling or legal recourse, according to the National Commission for Women (NCW).[92] Such information emphasises the necessity of an integrated approach to digital victim assistance that combines cyber forensic support, legal aid, and psychological care.

C. SOCIAL STIGMA, UNDERREPORTING, AND DIGITAL LITERACY GAPS

Underreporting is a widespread problem in the fight against cyber-gender violence. Because of social stigma, institutional indifference, and fear of character assassination, victims frequently choose not to file complaints.[93] Similar to the historical underreporting of sexual violence, this phenomenon is exacerbated online, where the line separating private and public humiliation dissolves in an instant.

According to empirical research, many Indian victims of online abuse turn to self-censorship or digital withdrawal, while less than 25% report the incident to the appropriate authorities.[94] Silence and impunity are reinforced by the patriarchal moral code, which frequently holds victims accountable for "inviting" online harassment. This victim-blaming culture runs counter

---

[90] *World Health Org., Constitution of the World Health Organisation, pmbl. (1946).*
[91] *X v. Health & Family Welfare Dep't, Gov't of NCT of Delhi*, (2022) 10 S.C.C. 1, ¶¶ 89–91 (India).
[92] National Commission for Women, *Annual Report 2022–23*, at 141–144 (2023).
[93] Ranjana Kumari, *Gendered Silences in Cyberspace: A Study on Underreporting of Online Abuse*, **Centre for Social Research Report** 7–9 (2020).
[94] United Nations Office on Drugs & Crime, *Global Study on Cyber Violence Against Women and Girls* 16–18 (2021).

to the equality and fraternity enshrined in the Preamble and is a social failure of constitutional morality.[95]

Gender vulnerability is further exacerbated by disparities in digital literacy. In India, only 33% of women and 57% of men report regularly using the internet, according to the National Family Health Survey (NFHS-5).[96] Women are unable to adequately protect themselves or seek remedies due to a lack of knowledge about privacy tools, reporting procedures, and legal rights. Achieving digital substantive equality under Articles 14 and 15 requires closing this digital divide.

D. THE ROLE OF LAW ENFORCEMENT, MEDIA, AND CIVIL SOCIETY

The institutional response to gender violence in cyberspace is still disjointed. Technological obstacles and jurisdictional complexities hinder investigations, and police frequently lack cyber-forensic training.[97] Although social media platforms are required by the Intermediary Guidelines and Digital Media Ethics Code, 2021, to remove offensive content upon notice, enforcement of these laws is patchy and unclear.[98] Law enforcement organisations must implement gender-sensitive initiatives that combine digital literacy and constitutional ethics.

The media and civil society organisations have two roles. On the one hand, they use campaigns like #JusticeForWomenOnline and #DigitalSafetyNow to increase advocacy and awareness. However, careless reporting or sensationalism can undermine privacy and worsen trauma. Therefore, legal reform must be complemented by ethical journalism that is based on consent and dignity.[99]

According to international human rights doctrine, states must take "due diligence" in preventing, looking into, and punishing gender-based violence, including that which takes place online.[100] Realising a constitutional ecosystem of cyber justice requires domestic adherence to this standard as well as collaborations between state institutions, tech companies, and civil society.

---

[95] *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1, ¶¶ 116–118 (India).
[96] Ministry of Health & Family Welfare, *National Family Health Survey (NFHS-5), 2019–21*, Vol. I, at 556–557.
[97] National Crime Records Bureau, *Crime in India 2022: Statistics*, Ministry of Home Affairs, Gov't of India, at 514–516 (2023).
[98] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Extraordinary, Part II, Sec. 3(i), Rule 3(2)(b).
[99] Press Council of India, *Norms of Journalistic Conduct*, ¶¶ 1.1–1.3 (2022).
[100] U.N. Hum. Rts. Council, *Due Diligence Framework on Violence Against Women*, U.N. Doc. A/HRC/23/49, ¶¶ 13–17 (2013).

CHAPTER-VIII THE FUTURE OF DIGITAL CONSTITUTIONALISM

A constitutional rethink of digital governance is required due to the evolution of cyberspace. The state's approach to cyber regulation must be guided by India's constitutional morality, which is based on liberty, equality, and fraternity. Laws, regulations, and technological advancements must all work together to protect women's autonomy, privacy, and involvement in digital life, according to a gender-sensitive digital constitutionalism.[101]

In order to harmonise the IT Act of 2000, the Bharatiya Nyaya Sanhita of 2023, and the Digital Personal Data Protection Act of 2023, legislative reforms must acknowledge cyber gender violence as a separate offence category.[102] In order to guarantee that online harms are regarded as constitutional violations rather than just criminal offences, courts should keep extending Article 21 to include digital dignity.[103] For survivors, a dedicated Cyber Gender Tribunal could guarantee restorative justice and speed up redress.

Multi-stakeholder cooperation is crucial in terms of policy. While the state must operationalise due diligence obligations through victim support, cyber awareness, and mental health programs, tech platforms must also bear enforceable duties of care.[104] Together, academia, media, and civil society form digital democracy's moral conscience, bringing the ideals of the constitution to life. India must essentially transition from a cyber-policing regime to one of cyber-constitutionalism, in which the egalitarian spirit of the Republic is reflected in digital spaces.

CHAPTER-IX CONCLUSION

Cyber gender violence is a constitutional challenge to justice, equality, and dignity in the digital republic rather than a side issue of online misconduct. Through its transformative ethos, the Indian Constitution aims to create a society in which advancements in technology enhance human freedom rather than jeopardise it.[105] The state affirms that every woman's digital safety is essential to her citizenship by establishing cyber regulation on the moral foundation of the constitution.

---

[101] Gautam Bhatia, *Digital Constitutionalism and the Indian State*, **Indian L. Rev.**, Vol. 6, No. 2, at 189–92 (2022).
[102] Information Technology Act, No. 21 of 2000 (India); Bharatiya Nyaya Sanhita, No. 45 of 2023 (India); Digital Personal Data Protection Act, No. 22 of 2023 (India).
[103] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1, ¶¶ 297–302 (India).
[104] U.N. Hum. Rts. Council, *Report of the Special Rapporteur on Freedom of Expression and Gender Justice*, U.N. Doc. A/HRC/47/25, ¶¶ 48–52 (2021).
[105] *Navtej Singh Johar v. Union of India*, (2018) 10 S.C.C. 1, ¶¶ 116–118 (India).

Harmonising ethics, technology, and law under the aegis of human dignity is necessary for the future. Constitutional morality thus becomes both a philosophy of governance and a practical tool mandating the state, judiciary, and digital corporations to co-create a cyberspace governed by empathy, accountability, and equality.[106] India's constitutional promise won't fully translate from text to technology until women can live in digital spaces without fear or silence.

[106] *Joseph Shine v. Union of India*, (2019) 3 S.C.C. 39, ¶¶ 124–126 (India).