Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey



# Cyber Misogyny and the Inadequacy of India's Legal Response

Andrea Gracelyn[a]

[a]Christ University Bangalore, India

*Received* 05 May 2026; *Accepted* 06 June 2026; *Published* 10 June 2026

*Cyber misogyny is often dismissed as an insignificant and virtual phenomenon. The gender-based harassment, abuse, and violence directed at women and girls through digital infrastructure represents not multiple individual incidents but a collective campaign that India's existing legal framework is fundamentally ill-equipped to address as a separate legal offence. This article analyses the vicarious gaps of India's legislation, specifically the Information Technology Act 2000, the Bharatiya Nyaya Sanhita 2023, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, and the Telecommunications Act 2023. It argues that these frameworks, constructed on an individual-offender morality model rooted in societal standards rather than a dignity-based framework, are incapable of handling the coordinated and structural nature of online gender-based violence against women. Through a conduct-based analysis of attacks such as non-consensual intimate image sharing, doxxing, deepfakes, and matrimonial surveillance technology, the article demonstrates that current provisions provide women with protection in theory; however, their practical application often results in either delayed or incomplete justice. This paper also draws on comparative frameworks from the United Kingdom's Online Safety Act 2023, the European Union's Digital Services Act 2022, Australia's Online Safety Act 2021, and India's obligations within CEDAW's General Recommendation No. 35. The article presents the recommendation of a dedicated cyber gender-based violence statute. Such legislation must identify cyber misogyny as a distinct legal category, impose specific platform duties with enforceable timelines, and provide civil remedies accessible independently of criminal prosecution.*

**Keywords:** *cyber misogyny, gender-based violence, harassment.*

## INTRODUCTION

Cyber misogyny refers to the various forms of gendered hatred, harassment, and abusive behaviour targeted at women and girls via the Internet.[1] Here is what separates it from mere 'cyber bullying', this form of hatred and or violence directed towards women and girls. While cyber bullying focuses on the broader sense of harassment, irrespective of sex or gender. Such behaviour is justified through structures such as the patriarchy and the more recently emerged 'manosphere' on the internet. The manosphere portrays women as manipulative and the idea of feminism as dangerous, which then leads to the justification of violence and hatred spread through organised online campaigns that promote stalking and hate speech.

**Cyber misogyny is most commonly seen in the following actions:**

1. Cyberstalking
2. Gender based hate speech through videos and articles
1. Non-consensual sharing of intimate images
2. Deepfakes or digitally altered images
3. Child sexual exploitation[2]

In India, Cyber misogyny is addressed indirectly through the Information Technology (IT) Act 2000 and the Bhartiya Nyaya Sanihita (BNS) 2023. Laws such as Section 354D (cyberstalking), Section 354A (sexual harassment, including showing pornography against a woman's will) and Section 66E (violation of privacy), Section 67/67A (publishing obscene or sexually explicit material), Section 67B (child pornography), Section 66C (identity theft) and Section 72 (breach of privacy) of the IT Act address a majority of the concerns. Recent amendments proposed in the IT Act also serve to include rules to better handle deepfakes on internet platforms.[3] However, the very structure of these provisions fails to look at the bigger picture. The law understands these offences as individual events - the offender vs the victim. But, most often, such behaviour is not an individual offence; it is almost always backed by a

[1] Nicole Etherington, 'Cyber Misogyny' (*Learning Network*) <www.gbvlearningnetwork.ca/our-work/briefs/brief-28.html> accessed 28 April 2026
[2] *Ibid*
[3] Vineet Upadhyay, 'India's new 3-hour deepfake removal rule: Experts urge strict compliance' *The Indian Express* (17 February 2026) <https://indianexpress.com/article/legal-news/indias-new-3-hour-deepfake-removal-rule-experts-urge-strict-compliance-10528122/> accessed 28 April 2026

system, a group of men that gain support and traction from each other for committing such offences. This gendered condition of online life is displayed through multiple doxxing and harassment attempts, all from different men targeting the same woman. The question of how she may seek legal relief against an entire community and how legislation must focus on the regulation of such committees is the main issue of this paper.

## CRITIQUE OF EXISTING FRAMEWORKS

**The IT Act 2000 and its Amendments: Drafted Blind to Gender:** The IT Act was drafted primarily to facilitate e-commerce transactions and to criminalise property-directed cybercrimes. Section 66A criminalised the sending of information that was considered 'grossly offensive' or caused 'annoyance' before its removal in the case of Shreya Singhal v Union of India. Instead of being used for its original purpose of protection, the section allowed the law to arrest those who dissented politically or posted mere satire, including women who themselves made use of the online space.[4] Though the Supreme Court's decision was backed by the constitution under Articles 19 and 21, the invalidation of this law led to a significant gap, especially in relation to gender-based harm.

Section 66E addresses the violation of privacy through the capture, publication or transmission of images of a person's private parts without consent. However, this struggles to truly provide justice when handling Non-Consensual Intimate Image Abuse (NCII). The requirement here is that the image must contain the presence of a private part. If the victim is captured in an intimate or compromising position but without meeting the criteria, the law remains silent on the same. Moreover, it does not provide any restriction against the sharing of images that once had the consent of the woman, considering it a transmission of obscenity over breach of privacy under Section 67A that criminalises the publication of sexually explicit material in electronic form.[5] The absence of strict timelines and adequate civil remedies makes this law not supportive of the fight against gender-based harm.[6]

**BNS Provisions and the Continuity of Colonial Morality:** The Bharatiya Nyaya Sanhita 2023 replaced the Indian Penal Code 1860, but the provisions governing gender-based harm

[4] *Shreya Singhal v Union of India* (2015) 5 SCC 1
[5] Dr. Karnika Seth, *COMPUTERS, INTERNET AND NEW TECHNOLOGY LAWS* (LexisNexis 2021)
[6] Pavan Duggal, *CYBERLAW: THE INDIAN PERSPECTIVE* (Saakshar Law Publications 2002)

have been carried forward instead of being reconceptualised.

Section 354A BNS, which addresses sexual harassment, including the showing of pornography against a woman's will, retains the essential structure of its predecessor.[7] The provision criminalises specific acts such as demand for sexual favours, making sexually coloured remarks, but does not account for the systemic pattern of conduct that constitutes cyber misogyny as a collective campaign. Section 354D BNS, which addresses stalking, fares somewhat better in its digital application as it explicitly includes electronic communication within its framework.[8] But this model of stalking is still focused on the individual instances; it refers to a single person repeatedly contacting or following a single victim. When the 'stalker' is instead a network of accounts engaging in both collective and synchronised harassment, the provision's requirements become nearly impossible to hold the network, the organiser, or the platform accountable.[9]

More fundamentally, the BNS's failure to shift from a morality-based to a dignity/autonomy-based framework for such gender offences means that the interpretation of the same by courts relies more on the harm done to feminine modesty and social reputation rather than to the individual woman's right to exist, speak and participate in public life without violence. This narrative leads to consequences such as a judge considering an assessment of the woman's conduct on social media as relevant to the assessment of harm done to her.[10] This, however, leads to the online violence being viewed as one where the mistake does not fall solely on the perpetrator, but rather that it is a result of a woman's platform and conduct on social media.

**Platform Liability Under the IT (Intermediary Guidelines) Rules 2021:** The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 represent India's most recent attempt to impose obligations on platforms operating within its jurisdiction. The Rules require significant social media intermediaries (SSMIs) to appoint grievance officers, acknowledge complaints within 24 hours, and resolve them within 15 days.[11] In practice, the grievance officer mechanism has been a significant failure for women complainants. Officers

[7] Indian Penal Code 1860, s 354A
[8] Indian Penal Code 1860, s 354D
[9] *The State of West Bengal v Animesh Boxi @ Ani Boxi @ Ani Bakshi* CRM No 11806/2017
[10] Ratanlal and Dhirajlal, *The Indian Penal Code* (35th edn, LexisNexis 2017)
[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

are appointed by the platform, report to the platform, and apply the platform's own community standards, which may not apply to the generalised agenda of gender violence.

Section 79 of the IT Act operates on a narrow, transaction-based model of 'notice-and-takedown.' This framework is structurally incapable of addressing the systemic and distributed nature of coordinated gendered harassment campaigns such as pile-ons or targeted trolling. Once again, the issue is tackled as an individual case and does not account for systemic backgrounds.[12]

**The Telecommunications Act 2023: A Missed Opportunity:** The Telecommunications Act 2023 has been presented as a comprehensive modernisation of India's telecommunications framework. In the context of cyber misogyny, it is a missed opportunity; the Act's definition of 'telecommunication services' encompasses the transmission of messages, voice, data, and other forms of communication across networks, but its regulatory services are restricted to the infrastructure of transmission and the entities that own and operate it.[13] This rigid, legal separation between carriage (transmission infrastructure) and content(the data being transmitted) fundamentally immunises the telecom framework from addressing issues like gendered digital violence.

It says nothing about content, nothing about platform obligations, nothing about gendered harm. The gap between 'communication' and 'content' is precisely where cyber misogyny lives. A deepfake video transmitted across a telecommunications network is regulated at the moment of transmission only until the network provider is subject to licensing conditions: the content of that transmission, the harm it causes, and the obligation to prevent its creation and distribution fall entirely outside the Act's framework. To simplify this, the act addresses the pipe but not the water that flows through it.

## SPECIFIC CONDUCT-BASED ANALYSIS

**Non-Consensual Intimate Image Sharing: The Legislative Vacuum:** Non-consensual intimate image (NCII) sharing is perhaps the form of cyber misogyny for which India's legislative vacuum is most clearly documented. The United Kingdom's Online Safety Act

[12] Apar Gupta, 'Liability of Intermediaries in India – From Troubled Waters to Safe Harbours' (2007) 13(2) Computer and Telecommunications Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1682468> accessed 28 April 2026
[13] Telecommunications Act 2023

2023 created a separate offence for sharing intimate images without consent, carrying a maximum sentence of two years and a separate offence for threatening to share such images.[14] Australia's Online Safety Act 2021 provides for a removal notice mechanism capable of compelling platforms to remove material within 24 hours.[15] India's response, however, is obtained by using sections 67 and 67A of the IT Act, which address the publication of obscene or sexually explicit content and do not require proof of non-consent as a distinct element. Along with this, sections 354A and 354D of the Bhartiya Nyaya Sanhita (BNS), which address harassment and stalking without any specific provision designed for image-based abuse.[16] Courts have attempted to apply these provisions creatively, but the results are inconsistent. Deepfake technology introduces a further dimension that the existing framework cannot reach at all. A deepfake image is considered manufactured, so the presence of consent, as mentioned within the framework of the act, becomes irrelevant. India has no provision that directly criminalises the manufacture and distribution of deepfake pornographic content targeting identified individuals and the proposed amendments to the IT Rules that have been proposed do not fill this gap in any systematic and adequate way.[17]

**Doxxing and Location-Based Threat:** Doxxing, i.e., the publication of a target's private identifying information, such as home address, workplace, phone number, family members' identities, is the mechanism by which cyber misogyny is most directly converted into a physical threat. A pile-on or collective campaign accompanied by doxxing is not merely an online harassment campaign; it is an invitation to offline violence.[18] Yet India has no standalone doxxing prohibition; rather, it is governed bleakly by stalking provisions under section 354D and criminal intimidation under section 351 of the BNS, or breach of privacy under section 72 IT Act. None of these was specifically designed to cause harm by publishing identifying information to facilitate third-party violence.

The problem is worsened by the anonymity and jurisdiction challenges that attend most doxxing cases. The person who publishes a woman's home address may be operating from outside India, using a VPN on a platform that routes traffic through multiple jurisdictions. India's existing framework provides no mechanism for speedy cross-border information

[14] Online Safety Act 2023
[15] Online Safety Act 2021
[16] Information Technology Act 2000, ss 67 and 67A
[17] Danielle Keats Citron, *HATE CRIMES IN CYBERSPACE* (Harvard University Press 2016)
[18] 'What Is Doxing?' (*Fortinet*) <www.fortinet.com/resources/cyberglossary/doxing> accessed 28 April 2026

requests, no mutual legal assistance treaty and no civil injunction mechanism available to a woman whose address has been published without her waiting for the criminal process to move at its ordinary pace, which has severe consequences due to time delay.

**Matrimonial Surveillance Technology:** A category of cyber misogyny that receives almost no legislative attention in India is the deployment of commercially available spyware and tracking technology within intimate relationships. Products marketed explicitly for spousal monitoring that enable one partner to read the other's messages, track their location in real time and access their call logs without detection are legally available in India, and their use is not specifically criminalised.

The IT Act's provisions on unauthorised access (section 43) and identity theft (section 66C) can theoretically apply to some instances of matrimonial surveillance, but the consent framework of these provisions is complicated by the legal and social norms of marriage in India, which, in line with history, treat spousal privacy, especially that of a woman, with suspicion. The Protection of Women from Domestic Violence Act 2005 does not address digital surveillance as a form of domestic abuse. In addition to that, there exists no judicial guidance system that considers such surveillance as domestic abuse.[19]

## INTERNATIONAL DIMENSIONS

**Comparative Legislative Models:** Three international frameworks aid this analysis as comparative benchmarks: the United Kingdom's Online Safety Act 2023, the European Union's Digital Services Act 2022, and Australia's Online Safety Act 2021. The UK Online Safety Act 2023 represents the most comprehensive statutory provision with relation to online gender-based harm in the common law world. It creates a standalone offence of sharing intimate images without consent, imposes safety duties on platforms, including risk assessments and proactive measures to protect women from harassment and a solid regulatory regime to further protect users.[20] The EU Digital Services Act 2022 takes a systemic risk approach to platform regulation. Very large online platforms are required to identify, assess, and proactively avoid systemic risks arising from their services, including risks to gender equality and the safety of women.[21] Australia's Online Safety Act 2021 is notable for

[19] Protection of Women from Domestic Violence Act 2005
[20] Online Safety Act 2023
[21] Digital Services Act 2022

its emphasis on a non-criminal civil regulatory model administered by the E- Safety Commissioner, an independent office with the power to issue removal notices to platforms and service providers, conduct investigations and impose civil penalties.[22]

**CEDAW and India's International Obligations:** Now, upon analyzing The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) Committee's General Recommendation No 35 (2017), which updates General Recommendation No 19 on violence against women, explicitly addresses technology-facilitated gender-based violence. It requires state parties to take legislative and regulatory measures to prevent, investigate and provide remedies for such violence, and specifically identifies online harassment and non-consensual intimate image (NCII) as a form of gender-based violence against women falling within the Convention's framework. India is a party to CEDAW, and under General Recommendation No 35 has obligations to ensure that its legal framework protects against technology-facilitated violence against women. The analysis in Parts II and II above demonstrates that India's current framework does not meet this standard.

## RECOMMENDATIONS

**The Case for a Dedicated Cyber Gender-Based Violence Statute:** The analysis establishes that the inadequacy of India's response to cyber misogyny is not a matter of drafting gaps that can be filled by amendment. It is a structural problem produced by a foundational error that is the treatment of cyber misogyny as individual, unrelated incidents rather than structural gender-based violence. This has produced a patchwork that cannot merely be fixed by filling the gaps; the appropriate response is a dedicated statute on cyber gender-based violence that retells the problem as a structural issue and builds principles around it.

Such a statute must contain the following elements at a minimum.

A solid framework that identifies cyber misogyny as a distinct category of gender-based violence and also defines each form of conduct, such as non-consensual intimate images, coordinated harassment, doxxing, deepfake abuse and matrimonial surveillance with both specificity and precision. It must treat cumulative and campaign conduct as a legally cognisable offence in addition to individual acts.

[22] Online Safety Act 2021

Second, a clear platform duty-to-act schedule with specific timelines that can include the following:

a. 24 hours for non-consensual intimate images (NCII) removal.
b. 48 hours for doxing.
c. 72 hours for reporting on coordinated harassment investigations. This should be backed by civil penalties for non-compliance administered by a specialist regulator.
d. An ex parte takedown mechanism available to complainants without the requirement to first complete a criminal First Information Report (FIR) process.
e. Fourth, a civil compensation system that operates independently of criminal prosecution, with the reversed burden of proof on platforms that have been notified of content and failed to act within prescribed timelines.
f. Fifth, a national registry of repeat platform violators and platforms that have received civil penalties above a threshold, whose regulatory status can be downgraded and subject to enhanced scrutiny.

**Platform Design Obligations as a Legal Category:** Beyond content removal, a structurally adequate response to cyber misogyny must engage with platform design, such as the founding choices that determine how harassment is amplified, how coordinated behaviour is detected, and how privacy defaults are set. This section seeks to promote platform design obligations as a distinct legal category.[23]

The legislative challenge is to impose design obligations without creating a censorship mandate. This is achievable in the following way, for example, instead of specifying what design choices platforms must make, a statute could specify the outcomes platforms must achieve, such as a reduction in coordinated harassment to below a specified threshold, removal of non-consensual intimate images (NCII) within prescribed timeframes and accessible blocking tools meeting specified usability standards. By allowing platforms to choose their own technical means of meeting those outcomes, the DSA's systemic risk approach is followed, and it becomes adaptable to India's constitutional and regulatory environment.[24]

[23] Online Safety Act 2021
[24] Digital Services Act 2022

## CONCLUSION

India's legal response to cyber misogyny fails because it was not designed to accommodate such a crime. Built from provisions drafted for different purposes, and it being a morality-based rather than a dignity-based framework for gender harm proves to be a significant obstacle. It being structured around an individual-offender model that does not consider coordinated and platform-mediated violence leaves women with a theoretical right to protection and a practical absence of remedy. The Telecommunications Act 2023 did not improve this picture, while the BNS did not transform it, and an amendment of the IT Act provisions will not resolve it.

This article has argued that structural problems require structural solutions. Cyber misogyny must be named as a distinct legal category, a form of structural gender-based violence that uses digital infrastructure to attack women for visibility and expression. That naming must be translated into a dedicated statutory reform that caters to platform accountability and also makes provisions for speedy justice and timelines when dealing with cases that require urgent action, like that of doxxing or non-consensual intimate images (NCII).

The models examined above, the UK's Online Safety Act, the EU's Digital Services Act, and Australia's E -Safety framework, demonstrate that this kind of legislative response is feasible within governance systems. India's legislation is capable of making such a change, but the will, both jurisprudential and societal, is required to ensure its smooth functioning. The urgency and importance with which the concerns of women harmed by this systemic attack are treated, the safer it becomes for them to have autonomy in their social presence, just as it should be.