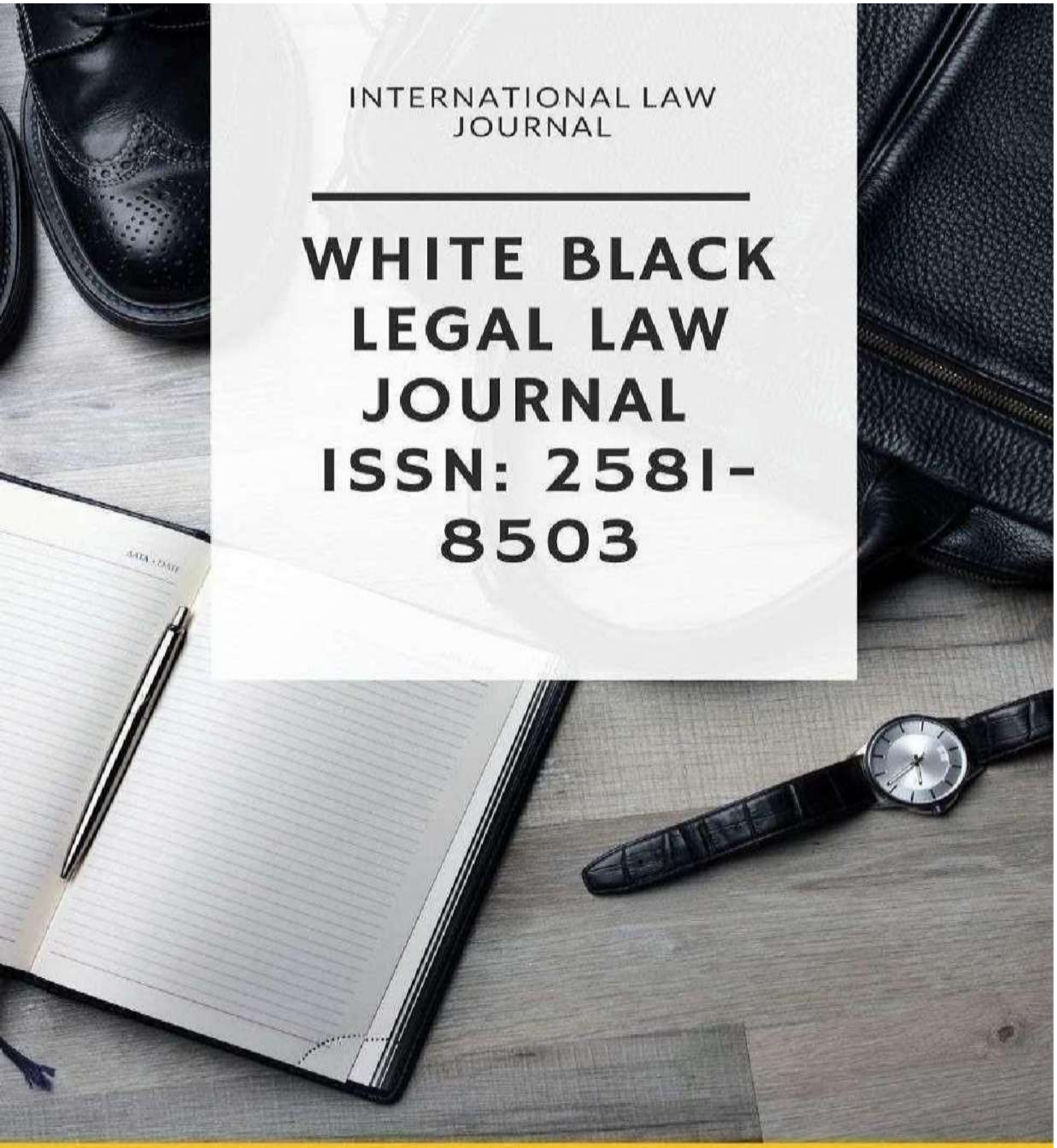

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CYBER FEMINISM AND ONLINE GENDERED VIOLENCE IN INDIA: A LEGAL ANALYSIS

AUTHORED BY - PRASHANT KUMAR CHAUHAN

Abstract

The proliferation of digital platforms and artificial intelligence-driven ecosystems has fundamentally transformed the landscape of gendered violence, exposing women and marginalized gender identities to unprecedented forms of online harm. In India, the intersection of patriarchal social structures, inadequate legal frameworks, and technologically sophisticated platforms has created a crisis of online gendered violence that existing cyber law has proven ill-equipped to address. This article critically examines the relationship between cyber feminism, constitutionalism, cyber law, platform governance, and artificial intelligence in the context of online gendered violence in India. Drawing upon feminist jurisprudence, constitutional law, digital governance scholarship, and comparative international legal frameworks, the article advances the argument that India's current cyber legal regime spanning the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023 remains structurally insufficient to counter technologically evolving forms of digital violence, including deepfake abuse, algorithmic amplification of misogyny, synthetic media exploitation, and platform-enabled harassment. The methodology is doctrinal, comparative, and interdisciplinary, incorporating constitutional analysis, case law review, and feminist legal theory. The article finds that the absence of a rights-based, feminist regulatory architecture, combined with weak platform accountability norms and inadequate judicial mechanisms, perpetuates systemic impunity. It recommends a comprehensive feminist cyber governance model grounded in constitutional dignity, platform transparency, and AI accountability. The article concludes that achieving gender justice in cyberspace requires a paradigm shift from reactive penalization to proactive structural reform.

Keywords: Cyber feminism; online gendered violence; deepfake abuse; platform accountability; digital constitutionalism; feminist jurisprudence; intermediary liability.

I. Introduction

The advent of the internet and digital communication technologies was initially heralded as a transformative force for gender equality a space where women could transcend physical limitations, access information freely, build solidarity networks, and participate in public discourse on equal terms. Cyber feminism, as a theoretical and activist movement emerging in the early 1990s, embraced this optimistic vision, positing that cyberspace offered women liberation from embodied patriarchal constraints. However, the digital revolution has produced a deeply paradoxical outcome: while women's participation in digital spaces has expanded significantly, so too has the scope, severity, and sophistication of gender-based violence online.

In India, this paradox is particularly acute. With over 850 million internet users as of 2025 and rapidly expanding mobile internet penetration, Indian women are increasingly present in digital spaces as content creators, professionals, activists, students, and citizens. Yet this presence is accompanied by pervasive online gendered violence in forms ranging from cyberstalking, trolling, and sexual harassment to deepfake pornography, doxxing, non-consensual image sharing, and coordinated mob harassment campaigns. The National Crime Records Bureau consistently reports significant increases in cyber crimes against women, though experts widely acknowledge that official statistics represent a fraction of actual incidence due to persistent underreporting.[1]

The legal framework governing this space has evolved incrementally. The Information Technology Act, 2000 the foundational statute governing cyberspace in India was designed primarily for data protection and e-commerce facilitation rather than the prevention of gendered digital violence.[2] Subsequent legislative interventions, including the Bharatiya Nyaya Sanhita, 2023 (BNS),[3] the Digital Personal Data Protection Act, 2023 (DPDPA),[4] and the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[5] have attempted to address emerging challenges, but fundamental gaps remain. These gaps are particularly pronounced in the context of artificial intelligence-generated abuse deepfakes, synthetic sexual imagery, and algorithmically amplified hate where existing legal categories struggle to achieve

[1]National Crime Records Bureau, Crime in India 2023, at 143-147 (Ministry of Home Affairs, Govt. of India, 2024).
[2]Information Technology Act, No. 21 of 2000, pmbl. (India).
[3]Bharatiya Nyaya Sanhita, No. 45 of 2023, pmbl. (India).
[4]Digital Personal Data Protection Act, No. 22 of 2023, pmbl. (India).
[5]The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).

adequate characterization and enforcement.

This article is animated by three research questions. First, does India's current cyber legal framework adequately address the technological evolution of online gendered violence, particularly AI-generated forms of abuse? Second, how do constitutional guarantees of dignity, equality, privacy, and non-discrimination bear upon the regulatory obligations of the state and platforms toward victims of online gendered violence? Third, what does a feminist, rights-based, and constitutionally grounded reform framework for cyber governance look like in the Indian context? The central hypothesis advanced is that India's present legal architecture suffers from a dual failure structural inadequacy in its substantive norms and enforcement deficits in its implementation mechanisms which together produce a governance vacuum that platforms exploit through algorithmic indifference and intermediary immunity.

The research methodology is primarily doctrinal and comparative, employing constitutional analysis, statutory interpretation, judicial review of case law, and examination of comparative international frameworks from the European Union, the United Kingdom, the United States, and Australia. It is supplemented by insights from feminist legal theory, digital governance scholarship, and socio-legal studies. The scope of this article is limited to India's domestic legal framework and its engagement with international human rights norms, with comparative references used for reform benchmarking rather than prescriptive transplantation.

II. Conceptual and Theoretical Framework

Cyber feminism, as theorized by scholars including Donna Haraway and the VNS Matrix collective in the 1990s, initially represented a utopian convergence of feminist politics and digital technology a vision of cyberspace as a domain of fluid identities, decentralized power, and emancipatory possibility.[6] Sadie Plant's influential work characterized digital networks as inherently feminist structures, resistant to hierarchical control.[7] However, by the second decade of the twenty-first century, this optimism had given way to a more critical and pragmatic cyber feminist analysis that engaged directly with the reproduction of patriarchal power structures in digital environments. Contemporary cyber feminism is therefore best understood as a critical analytical and political stance that interrogates how gender inequality is reproduced, amplified,

[6]Donna Haraway, A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century, in Simians, Cyborgs and Women: The Reinvention of Nature 149 (1991).
[7]Sadie Plant, Zeros and Ones: Digital Women and the New Technoculture 37-41 (1997).

and institutionalized through technology.

Online gendered violence is an umbrella term encompassing a diverse spectrum of harmful behaviors perpetrated through digital mediums that disproportionately target individuals on the basis of their gender, gender identity, or sexual orientation. The Council of Europe defines technology-facilitated violence against women as acts perpetrated through information and communications technologies that result in, or are likely to result in, physical, sexual, psychological, or economic harm.[8] Within this broad category, cyber misogyny refers to systematic expressions of hatred, contempt, and discrimination against women in online environments, frequently operationalized through coordinated harassment campaigns, rape threats, and sexualized abuse. Cyberstalking involves the persistent electronic monitoring and harassment of an individual through digital means, often to instill fear or exercise control, and has been analyzed through criminological frameworks as an extension of intimate partner violence into digital space.[9]

Doxxing the deliberate exposure of a person's private information, including home address, workplace, and contact details, without consent functions as a mechanism of digital terror that often precedes or enables physical violence. Revenge pornography, or more accurately described as non-consensual intimate image sharing (NCII), involves the distribution of private sexual images without the subject's consent, typically by former intimate partners as a tool of humiliation and control. Clare McGlynn and Erika Rackley's conceptual framework of image-based sexual abuse (IBSA) captures the full range of non-consensual sexual image harms including deepfakes, upskirting, and voyeurism within a unified analytical and regulatory frame that foregrounds victim harm rather than perpetrator categorization.[10]

Deepfake abuse represents perhaps the most technically sophisticated and legally challenging form of online gendered violence. Deepfake technology, powered by generative adversarial networks and diffusion models, enables the creation of hyperrealistic synthetic media including pornographic images and videos superimposing a real person's likeness onto fabricated content without consent.[11] The majority of deepfake pornography targets women, including public

[8]Council of Europe, Mapping Study on Cyberviolence, Cybercrime Convention Committee, T-CY(2017)10, at 12 (2018).
[9]Danielle Keats Citron, Hate Crimes in Cyberspace 14-18 (2014).
[10]Clare McGlynn & Erika Rackley, Image-Based Sexual Abuse, 37 Oxford J. Legal Stud. 534, 537 (2017).
[11]Nina Schick, Deep Fakes and the Infocalypse: What You Urgently Need to Know 89-94 (2020).

figures, journalists, activists, and ordinary individuals. Algorithmic discrimination refers to the systematized reproduction of gender biases through automated systems, including content recommendation algorithms that amplify misogynistic content and predictive systems that disproportionately surveil marginalized communities.[12]

Platform patriarchy, a concept drawn from feminist political economy, describes the structural embedding of gendered power relations within digital platform architectures manifest in content moderation systems that consistently fail women, algorithmic amplification of misogynistic content, and governance frameworks designed without meaningful feminist input. Digital constitutionalism represents an emerging scholarly paradigm that applies constitutional values dignity, equality, free speech, due process to the regulation of digital platforms and algorithmic systems, recognizing that the technical architectures of private platforms increasingly exercise quasi-state power over public discourse and individual rights.[13] Feminist legal theory, in the tradition of scholars including Catharine MacKinnon, Patricia Williams, and Drucilla Cornell, challenges the ostensible neutrality of law and legal institutions, exposing how formal legal equality often reproduces substantive gender inequality.[14]

III. Constitutional and Human Rights Dimensions

The constitutional framework of India offers a foundational basis for regulating online gendered violence, though its full protective potential remains underutilized in cyber governance. Article 14 guarantees equality before law and equal protection of laws,[15] which must be understood as encompassing an obligation on the state to ensure that the legal system does not, through omission or inadequate design, produce discriminatory outcomes for women seeking redress in cyberspace. Article 15(1) prohibits discrimination on grounds of sex, and read in conjunction with Article 15(3) which permits special provisions for women creates a constitutional authorization for gender-specific cyber legislation that addresses the particularized harms women face online.[16]

[12]Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism 10-15 (2018) (applying the framework by analogy to gender-based algorithmic discrimination).
[13]Jack Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and the Future of Free Expression, 51 U.C. Davis L. Rev. 1149, 1185-1190 (2018).
[14]Catharine A. MacKinnon, Toward a Feminist Theory of the State 162-166 (1989) (theorizing the limits of formal legal equality in achieving substantive gender justice).
[15]India Const. art. 14.
[16]India Const. art. 15, cl. 1, 3.

Article 19(1)(a) guarantees freedom of speech and expression, and its protection has been central to debates about intermediary liability and content moderation.[17] However, as the Supreme Court affirmed in *Shreya Singhal v. Union of India*, this freedom is not absolute, and Article 19(2) permits reasonable restrictions in the interests of public order, decency, and the rights of others.[18] The challenge for feminist cyber governance is to navigate the tension between protecting free expression and protecting women from online violence a tension that demands context-sensitive, evidence-based regulatory design rather than blunt censorship.

Article 21, which guarantees the right to life and personal liberty,[19] has through judicial interpretation evolved into the most expansive constitutional provision in the Indian legal arsenal. The Supreme Court's landmark recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* has profound implications for online gendered violence privacy encompasses informational privacy, dignity, and bodily autonomy, all of which are violated by non-consensual image sharing, deepfake abuse, and doxxing.[20] Furthermore, the Court's recognition of the right to dignity as an essential component of Article 21 creates a constitutional imperative to protect women from online harassment that degrades and dehumanizes.

The doctrine of transformative constitutionalism, as elaborated by scholars including Karl Klare and developed in the Indian context through judgments like *Navtej Singh Johar v. Union of India,* holds that constitutions are not merely negative charters of constraint but positive instruments of social transformation demanding that the state actively dismantle structures of subordination.[21][22] Applied to cyber governance, transformative constitutionalism mandates not merely the penalization of individual acts of online violence, but the structural reform of platform governance, algorithmic design, and digital regulatory architecture to achieve substantive gender equality.

At the international human rights level, the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) obligates state parties, including India, to take all

[17]India Const. art. 19, cl. 1(a), 2.
[18]Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[19]India Const. art. 21.
[20]Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[21]Navtej Singh Johar v. Union of India, (2018) 10 SCC 1, pp.114-120 (Chandrachud, J., concurring) (articulating transformative constitutionalism in the Indian context).
[22]Karl Klare, Legal Culture and Transformative Constitutionalism, 14 S. Afr. J. Hum. Rts. 146, 150-155 (1998).

appropriate measures to eliminate discrimination against women in all forms.[23] The CEDAW Committee's General Recommendation No. 35 explicitly addresses gender-based violence as a form of discrimination and recognizes technology-facilitated violence as falling within the treaty's ambit.[24] The International Covenant on Civil and Political Rights (ICCPR) guarantees rights to privacy (Article 17) and equality (Article 26),[25] while the Universal Declaration of Human Rights (UDHR) enshrines dignity as the foundational value of the international human rights framework.[26] The United Nations Special Rapporteur on Violence Against Women has repeatedly called upon states to develop comprehensive legislative frameworks addressing technology-facilitated gender-based violence, including deepfake abuse, online harassment, and algorithmic discrimination.[27]

IV. Existing Legal Framework in India

The Information Technology Act, 2000 (IT Act) constitutes the primary legislative response to cybercrime and digital governance in India. Section 66E penalizes the violation of privacy through the capturing, publishing, or transmitting of private images without consent a provision that is partially applicable to non-consensual intimate image sharing, though it does not adequately address deepfake content or AI-generated synthetic imagery.[28] Sections 67 and 67A penalize the publishing of obscene and sexually explicit material in electronic form respectively, carrying imprisonment up to three years for first offences.[29] However, these provisions suffer from vagueness, evidentiary challenges, and interpretive inconsistencies that significantly limit their practical effectiveness in addressing the full spectrum of online gendered violence.

The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, contains provisions addressing voyeurism (Section 77), cyberstalking (Section 78), and sexual harassment (Section

[23]Convention on the Elimination of All Forms of Discrimination Against Women, art. 2, opened for signature Dec. 18, 1979, 1249 U.N.T.S. 13 (entered into force Sept. 3, 1981).
[24]CEDAW Committee, General Recommendation No. 35 on Gender-Based Violence Against Women, pp.20, U.N. Doc. CEDAW/C/GC/35 (2017).
[25]International Covenant on Civil and Political Rights, arts. 17, 26, opened for signature Dec. 16, 1966, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).
[26]Universal Declaration of Human Rights, pmbl., G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).
[27]Report of the Special Rapporteur on Violence Against Women and Girls, Technology-Facilitated Gender-Based Violence Against Women, pp.12, U.N. Doc. A/HRC/53/36 (2023).
[28]Information Technology Act, No. 21 of 2000, s. 66E (India).
[29]Information Technology Act, No. 21 of 2000, s.s. 67, 67A (India).

75).[30] However, the BNS lacks any explicit provision addressing deepfake pornography, synthetic media abuse, or non-consensual image sharing in its comprehensive digital dimensions a significant legislative omission that reflects the failure to anticipate the pace of technological change. The absence of a standalone deepfake offence, in contrast to South Korea and the United Kingdom where specific legislation has been enacted,[31] represents a critical gap in India's cyber criminal law.

The Digital Personal Data Protection Act, 2023 establishes a framework for the protection of personal data and creates obligations on data fiduciaries including digital platforms to process data only for specified, consented purposes.[32] However, the DPDPA's enforcement architecture remains in nascent institutional form, and its remedial mechanisms do not directly address online gendered violence beyond data privacy violations. The Indecent Representation of Women (Prohibition) Act, 1986, predates the digital era and applies primarily to print and broadcast media, rendering it largely inapplicable to online content.[33]

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduced significant platform accountability obligations, including requirements for significant social media intermediaries (SSMIs) to appoint grievance officers, establish complaint redressal mechanisms, and proactively trace the originator of problematic content. However, the Rules have been criticized for simultaneously creating disproportionate surveillance risks and failing to establish meaningful intermediary liability for gender-based online violence. The safe harbor protection under Section 79 of the IT Act which insulates intermediaries from liability for third-party content so long as they comply with due diligence obligations continues to function as a substantial shield against platform accountability for online gendered violence, insulating platforms from civil claims even where they have demonstrably failed to act on reported content.[34]

Enforcement mechanisms remain critically underdeveloped. Cyber cells across Indian states are chronically under-resourced, lack gender sensitization training, and suffer from insufficient

[30]Bharatiya Nyaya Sanhita, No. 45 of 2023, s.s. 77, 78, 95 (India).
[31]South Korea, Act on Special Cases Concerning the Punishment of Sexual Crimes, art. 14-2 (2020) (criminalizing deepfake sexual content without consent); Online Safety Act 2023, c. 50, s. 188 (UK) (creating criminal offence of sharing intimate images without consent, including deepfakes).
[32]Digital Personal Data Protection Act, No. 22 of 2023, s.s. 8-11 (India) (data fiduciary obligations).
[33]Indecent Representation of Women (Prohibition) Act, No. 60 of 1986 (India).
[34]Information Technology Act, No. 21 of 2000, s. 79 (India) (intermediary safe harbor).

technical expertise to investigate AI-generated offences. CERT-In's mandate focuses on cybersecurity incident response rather than victim-centered remediation. Jurisdictional complexity arising from cross-border platform operations, server locations in foreign jurisdictions, and the anonymity afforded by VPNs and pseudonymous accounts creates substantial practical barriers to investigation and prosecution.

V. Judicial Trends and Case Law Analysis

The Supreme Court's landmark decision in *Shreya Singhal v. Union of India* (2015) struck down Section 66A of the IT Act as unconstitutional, holding that its vague and overbroad criminalisation of online speech violated Article 19(1)(a).[35] While this judgment was a significant vindication of digital free expression, its implications for online gendered violence are complex: the expansion of intermediary safe harbor protections and the invalidation of broadly worded content prohibitions created a regulatory vacuum that platforms have exploited, often at the expense of women's online safety. The judgment, while doctrinally correct in its free speech analysis, has had the unintended consequence of chilling legislative efforts to regulate online harmful speech without adequate constitutional scaffolding.

Justice K.S. Puttaswamy v. Union of India (2017) is transformative for cyber governance. The nine-judge bench's unanimous recognition of privacy as a fundamental right incorporating informational privacy, decisional autonomy, and dignity has direct implications for non-consensual image sharing, data exploitation, and platform surveillance.[36] The Court's articulation of contextual integrity as a component of informational privacy provides a constitutional foundation for challenging deepfake abuse, where a person's likeness is extracted from one context and inserted, without consent, into a degrading synthetic context.

Vishaka v. State of Rajasthan (1997), though not a cyber law case, established the critical precedent for judicial law-making in the absence of legislative action to protect women's dignity and safety.[37] The Vishaka guidelines prescribing institutional obligations for preventing and addressing sexual harassment were subsequently codified in the Prevention of Sexual Harassment at Workplace Act, 2013.[38] The same tradition of purposive judicial creativity is

[35]Shreya Singhal v. Union of India, (2015) 5 SCC 1, pp.93-107 (striking down s. 66A as unconstitutional).
[36]Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, pp.301-310 (Chandrachud, J.) (recognizing informational privacy and contextual integrity as fundamental rights).
[37]Vishaka v. State of Rajasthan, (1997) 6 SCC 241, pp.15-16 (laying down guidelines for prevention of sexual harassment in the absence of specific legislation).
[38]Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, No. 14 of 2013 (India).

available to courts addressing online gendered violence in the absence of comprehensive legislation, particularly in developing platform-specific accountability norms and interim relief mechanisms for victims of deepfake abuse.

Comparatively, United States jurisprudence under Section 230 of the Communications Decency Act has provided platforms near-absolute immunity from liability for user-generated content,[39] though the legislative interventions of FOSTA-SESTA (2018) carved out limited exceptions for sex trafficking facilitation.[40] European courts applying the Digital Services Act have imposed greater platform accountability obligations, including algorithmic transparency and expedited content removal for clearly illegal content. UK courts applying the Online Safety Act 2023 framework are developing jurisprudence on platform duty of care obligations. Australian tribunals applying the Online Safety Act 2021 have enforced removal orders for cyber abuse content, establishing important procedural precedents for administrative enforcement outside traditional criminal courts.[41]

VI. Social Media Platforms, Artificial Intelligence, and Platform Accountability

The contemporary landscape of online gendered violence is inseparable from the architectures of social media platforms Meta, Instagram, X (formerly Twitter), Telegram, and an expanding ecosystem of AI-generated content platforms. These platforms are not neutral conduits for user expression but active participants in shaping the information environment through algorithmic curation, engagement optimization, and content moderation systems that carry significant gender implications. As argued in the context of platform accountability and AI content moderation, platform governance under the UN Guiding Principles on Business and Human Rights demands that technology companies operationalize human rights due diligence frameworks that specifically account for gender-based harms.[42]

[39]47 U.S.C. s. 230 (2018) (Communications Decency Act, s. 230).
[40]Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA-SESTA), Pub. L. No. 115-164, 132 Stat. 1253 (2018).
[41]Online Safety Act 2021 (Cth) s.s. 36-38 (Austl.) (eSafety Commissioner removal notice and cyber abuse scheme).
[42]Prashant Chauhan, *Platform Accountability in the Age of AI in India: Reconciling Corporate Autonomy with Digital Human Rights Under the UNGPs Framework* (2025), available at https://www.researchgate.net/publication/400215025_Platform_Accountability_in_the_Age_of_AI_in_India_Reconciling_Corporate_Autonomy_with_Digital_Human_Rights_Under_the_UNGPS_Framework (last visited May 10, 2026).

The phenomenon of algorithmic amplification of misogyny represents one of the most structurally embedded forms of platform-facilitated gender violence. Research has documented how recommendation algorithms on major platforms systematically amplify content that sexualizes, demeans, or threatens women, because such content generates higher engagement metrics that platforms monetize through targeted advertising.[43] This is not incidental dysfunction but a product of platform capitalism's fundamental logic: maximizing attention and advertising revenue regardless of the human rights costs imposed on targeted communities. The gendered architecture of engagement algorithms constitutes what feminist scholars have termed "platform patriarchy" a structural embedding of masculine normative assumptions in the technical design of systems that govern online expression.[44]

Deepfake pornography has emerged as one of the most harmful applications of artificial intelligence in the context of gendered violence. As noted that examining AI governance and cybersecurity law in India, the regulatory framework has not kept pace with the capabilities of generative AI systems, including large language models and diffusion models that can produce synthetic sexual content of devastating realism.[45] Research indicates that the overwhelming majority of deepfake videos found online constitute non-consensual pornography, with women as the primary targets.[46] The harm caused by deepfake pornography is multidimensional: it violates privacy and dignity, silences victims through fear and shame, damages professional reputations, and constitutes a form of sexual violence that produces genuine psychological trauma even in the absence of physical contact.

Content moderation failures on major platforms follow a persistent pattern in relation to gendered violence. Meta's Oversight Board, while a notable institutional experiment in platform governance, lacks binding authority and has been criticized for inadequate attention to gender-based content harms. X's dismantling of trust and safety infrastructure following its 2022 acquisition has been widely documented, producing measurable increases in online harassment of women and marginalized groups. Telegram's encryption and minimal

[43]Global Witness & Access Now, Targeting Women Online: Platform Accountability and Algorithmic Amplification of Gender-Based Violence 22-27 (2024).
[44]Kate Klonick, The New Governors: The People, Rules, and Processes Governing Online Speech, 131 Harv. L. Rev. 1598, 1622-1627 (2018).
[45]Prashant Chauhan, AI-Powered Zero Trust Architecture and Cybersecurity Law in India, Int'l J. Juris. Sci. & Res. [IJJSR] (2024) (analyzing regulatory gaps in AI governance with reference to generative AI capabilities).
[46]Sensity AI, The State of Deepfakes 2023: Landscape, Threats, and Impact 8-12 (2023) (documenting that approximately 98% of deepfake videos online are non-consensual pornography, with women as primary targets).

moderation have made it a preferred platform for the distribution of non-consensual intimate imagery and coordinated harassment campaigns targeting women activists, journalists, and public figures.

Corporate accountability for platform-facilitated gendered violence must be understood through the lens of the UN Guiding Principles, which impose on corporations a responsibility to respect human rights, including through due diligence to identify, prevent, and mitigate adverse impacts on women's rights. The absence of a comprehensive framework integrating platform liability, algorithmic accountability, and victim remediation reflects a broader failure of governance design that existing law has been unable to remedy.

VII. Cyber Feminism as Resistance

Notwithstanding the pervasive harms of online gendered violence, digital space has also been a terrain of remarkable feminist resistance and political mobilization. The #MeToo movement, as it manifested in India in 2018, demonstrated the transformative potential of social media as a platform for survivor testimonies, collective accountability, and public naming of perpetrators including across legal, journalistic, and entertainment industries.[47] Indian women's use of Twitter, Instagram, and WhatsApp to organize, document, and disseminate information about gender-based violence represents a form of counter-hegemonic digital practice that directly challenges both offline patriarchy and online misogyny.

Feminist counter-publics a concept drawn from Nancy Fraser's critique of the bourgeois public sphere have found in digital platforms an institutional space for the formation of solidarity networks, the articulation of subordinated gender perspectives, and the coordination of political action.[48] Organizations including iCall, Point of View, and the Internet Freedom Foundation in India have combined digital literacy initiatives with feminist advocacy to support survivors of online gendered violence and advocate for legislative reform.[49] Academic and civil society documentation of deepfake abuse, doxxing campaigns, and platform failures has been indispensable in creating the evidentiary basis for policy reform and judicial intervention.

[47]Nivedita Menon & Vrinda Grover, Online, on Fire: #MeToo in India and the Feminist Legal Response, 54 Econ. & Pol. Wkly. 32, 35-38 (2019).
[48]Nancy Fraser, Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy, 25/26 Soc. Text 56, 66-68 (1990) (theorizing counter-publics as parallel discursive arenas).
[49]Internet Freedom Foundation, Online Violence Report: Mapping Digital Attacks on Women Journalists and Activists in India (2024).

Digital literacy, understood not merely as technical competence but as the critical capacity to navigate online spaces safely and exercise digital rights effectively, is an essential component of feminist resistance to online violence. However, digital literacy programs must be complemented by structural reforms in platform governance and legal regulation, lest the burden of preventing online violence be displaced entirely onto individual women a dynamics that feminist legal theorists identify as a form of victim-blaming institutionalized within regulatory design.

VIII. Comparative and International Approaches

The European Union's Digital Services Act (DSA, 2022) represents the most comprehensive platform accountability framework in operation as of 2025.[50] The DSA imposes risk assessment obligations on very large online platforms (VLOPs), requiring them to identify and mitigate systemic risks including gender-based violence amplification, and mandates algorithmic transparency, crisis response protocols, and independent audit requirements. The DSA's focus on systemic risk rather than merely individual content removal makes it a structurally superior framework for addressing the platform-level drivers of online gendered violence requiring platforms to examine and reform the architectural features that enable mass-scale harassment rather than responding reactively to reported content.

The United Kingdom's Online Safety Act 2023 introduces a duty of care framework for platforms, requiring them to proactively protect users from illegal content including intimate image abuse and from content that is harmful to women.[51] The Act's provisions on priority illegal content, including cyber flashing and non-consensual intimate image sharing, and its regulatory architecture centered on Ofcom as the enforcement regulator, provide a model for India's consideration. However, the Act has been criticized for insufficient protections for activist voices and for the complexity of its risk assessment obligations, which may prove disproportionately burdensome for smaller platforms.

Australia's Online Safety Act 2021 establishes the eSafety Commissioner as a specialized regulatory authority with powers to issue removal notices, investigate complaints, and enforce basic online safety expectations on platforms. Its cyber abuse scheme enables individuals

[50]Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act), arts. 26, 34-36, 2022 O.J. (L 277) 1.
[51]Online Safety Act 2023, c. 50, s.s. 10-12, 54-55 (UK) (duty of care and priority illegal content provisions).

targeted by serious cyber abuse to obtain removal orders through an administrative process that is significantly less burdensome than civil litigation a model particularly relevant to India's context of overburdened courts, high litigation costs, and pervasive underreporting of cyber crimes.[52] The eSafety Commissioner's approach of centering victim experience in regulatory design offers important pedagogical lessons for Indian regulatory architecture.

The United States' Section 230 immunity model has proven inadequate in protecting women from platform-facilitated violence, as its near-absolute intermediary immunity prevents victims from pursuing civil remedies against platforms for foreseeable harms.[53] India should resist the importation of the US model and instead draw primarily on the DSA and Australian regulatory frameworks as comparative references for reforming its own platform governance architecture. A contextually calibrated synthesis combining the DSA's systemic risk approach, the UK's duty of care framework, and Australia's administrative enforcement model offers the most promising template for India's reform efforts.

IX. Challenges in Existing Legal Remedies

The challenges confronting victims of online gendered violence seeking legal remedies in India are structural, procedural, and attitudinal. Underreporting is perhaps the most significant challenge: research consistently indicates that the vast majority of online gendered violence goes unreported, owing to victim blaming, stigmatization of survivors particularly in cases involving intimate imagery fear of retraumatization through the investigative process, and profound distrust of law enforcement institutions.[54] The cultural normalization of online harassment against women frequently dismissed as the inevitable cost of digital participation further suppresses reporting and embeds impunity within everyday platform experience.

Police insensitivity and technical incompetence represent compounding institutional failures. Gender-sensitive training in cyber crime investigation remains inadequate across most state police forces, and officers frequently respond to complaints of online violence with dismissiveness, advice to delete social media accounts, or interrogation of victims' behavior rather than systematic investigation of offenders. The procedural complexity of gathering

[52]eSafety Commissioner (Australia), Annual Report 2023-24, at 18-24 (2024) (documenting enforcement actions under the cyber abuse removal scheme).
[54]Ravi Shankar Prasad & Nidhi Razdan, Underreporting and Victim Stigma in Online Sexual Violence: Survey Evidence from Urban India, 12 J. Cyber L. & Info. Pol'y 45, 52-57 (2024).

digital evidence including platform data subject to foreign data protection laws, metadata from encrypted communications, and AI-generated content requiring forensic authentication places significant burdens on investigators that existing technical capacity often cannot satisfy.

Cross-border jurisdiction creates substantial challenges in cases where perpetrators operate from foreign jurisdictions, use anonymizing technologies, or exploit platforms headquartered outside India. Mutual legal assistance treaty mechanisms are slow and often ineffective for the rapid preservation of digital evidence.[55] Technological anonymity including VPNs, pseudonymous accounts, and distributed communication platforms significantly impedes the identification and prosecution of perpetrators. The AI-generated nature of deepfake abuse further complicates accountability: when harmful content is produced by AI systems rather than individual human perpetrators, existing criminal law frameworks focused on individual perpetrator liability struggle to achieve adequate characterization or enforcement.

X. Recommendations and Reform Framework

A feminist cyber governance model for India must begin from the constitutional recognition that women's equal enjoyment of digital spaces is a fundamental rights imperative, not a regulatory preference. This model demands structural reform across five dimensions: legislative, institutional, platform governance, remedial, and educational.

Legislatively, India requires a standalone Cyber Gendered Violence Act that comprehensively addresses deepfake pornography, non-consensual intimate image sharing, algorithmic harassment, doxxing, and AI-generated sexual abuse, with specific provisions for victim-centered remedies including swift content removal, anonymized reporting mechanisms, and civil damages. The Act should incorporate a definitional framework for image-based sexual abuse that is technologically neutral capable of capturing emerging forms of harm without requiring constant statutory amendment. The BNS should be amended to include explicit provisions on AI-generated gendered violence, adopting the legislative approach of South Korea and the United Kingdom in criminalizing deepfake pornography with meaningful penalties.

[55]Pavan Duggal, Cyber Law in India: A Critical Analysis 214-219 (5th ed. 2023) (noting the inadequacy of mutual legal assistance treaty mechanisms for expedited digital evidence preservation).

Institutionally, specialized cyber courts with gender-sensitive composition, training, and procedural norms should be established in each state, empowered to issue emergency preservation and removal orders against platforms, with jurisdiction over both criminal and civil claims arising from online gendered violence. A National Cyber Gender Violence Authority modeled partly on Australia's eSafety Commissioner should be established with a mandate to receive complaints, issue removal orders, conduct investigations, and publish annual transparency reports on platform compliance.

Platform accountability norms must be substantially strengthened. Significant social media intermediaries should be required to conduct mandatory gender-impact assessments of their algorithmic systems, proactively detect and remove non-consensual intimate imagery using automated hash-matching and AI detection tools, maintain transparent content moderation policies with gender-disaggregated data, and establish accessible victim reporting mechanisms with defined response times. The liability protection under Section 79 of the IT Act should be conditioned on demonstrable compliance with gender-sensitive due diligence obligations, creating meaningful financial incentives for platform intervention rather than passive tolerance of gendered harm.

AI accountability regulation must address the generative AI systems that produce deepfake content. Providers of generative AI models should be required to implement technical safeguards preventing the generation of non-consensual synthetic sexual imagery, maintain audit trails of content generation, and cooperate with law enforcement investigations. Victim compensation mechanisms, including a state-administered victim assistance fund for survivors of online gendered violence, should be established to provide immediate financial support for legal representation, psychological counseling, and technical assistance in evidence preservation. Gender-sensitive cyber policing requires mandatory training for all cyber crime officers in the gendered dimensions of digital violence, trauma-informed investigative practices, and technical capacity in AI forensics. Digital literacy initiatives, designed with feminist pedagogical principles and targeted particularly at women from rural, lower-income, and marginalized communities, should be scaled as part of India's Digital India program, ensuring that women acquire not merely technical skills but the critical capacity to exercise their digital rights, identify online threats, and access legal remedies.

The constitutional framework articulated above demands that these reforms be understood not

as discretionary policy choices but as obligations grounded in Articles 14, 15, 19, and 21, amplified by India's international human rights commitments under CEDAW, the ICCPR, and emerging UN digital rights frameworks.[56] Transformative constitutionalism, as a jurisprudential orientation, demands nothing less than the systematic dismantling of the legal and architectural structures that reproduce gender subordination in cyberspace.

XI. Conclusion

India's current cyber legal regime does not adequately protect women and marginalized genders from the evolving spectrum of online gendered violence. The structural inadequacies of the IT Act, the BNS, and the DPDPA compounded by institutional failures in enforcement, platform indifference amplified by intermediary immunity, and the technologically accelerating harms of AI-generated abuse collectively produce a governance vacuum that perpetuates systemic impunity for online gender-based violence.

The constitutional framework, properly understood through the lens of transformative constitutionalism and feminist jurisprudence, demands more than incremental reform. Articles 14, 15, 19, and 21 read in conjunction with India's obligations under CEDAW, the ICCPR, and emerging UN digital rights frameworks create a constitutional imperative for a feminist regulatory architecture that places victim dignity, platform accountability, and algorithmic justice at its center. The judicial creativity demonstrated in *Vishaka* and the constitutional imagination of *Puttaswamy* offer doctrinal resources for courts and legislators alike to construct that architecture in the absence of comprehensive legislative action.

Cyber feminism, as both a theoretical framework and a political practice, offers indispensable resources for this reform agenda insisting not merely on formal legal equality but on the substantive transformation of the technical, institutional, and cultural structures that reproduce gender subordination in digital space. The promise of constitutional democracy in the digital age must be measured not only by the rights it formally guarantees but by the structural conditions it creates for their equal enjoyment. As the scholarship on platform accountability and AI governance has argued, the responsible development of digital ecosystems requires that human rights including women's rights be operationalized as non-negotiable design constraints

[56]Gabrielle Appleby & Anna Olijnyk, Transformative Constitutionalism and Gender Justice in the Digital Age, 47 Fed. L. Rev. 189, 201-208 (2025).

rather than post-hoc compliance obligations.

The future of gender justice in cyberspace lies not in the periodic criminalisation of new forms of online harm as they emerge, but in the construction of a proactive, feminist, constitutionally grounded digital governance architecture one that holds platforms structurally accountable, empowers victims with accessible remedies, and treats the equal digital citizenship of women not as an aspiration, but as a constitutional guarantee that the law is obligated to realize.