

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

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

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

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

Digital Violence Against Women: An Emerging Challenge in Indian Law

KAVIYA K* AND MEENATCHI M**

ABSTRACT

The proliferation of digital technologies has transformed the nature, scale, and reach of violence against women, giving rise to a distinct category of harm now widely described as "digital violence" or "technology-facilitated gender-based violence." This manuscript examines the adequacy of India's legal architecture, spanning the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, together with its 2025 and 2026 amendments, in confronting this emerging challenge. It traces the evolution of judicial responses, from foundational rulings on cyber-obscenity and intermediary liability to the recent surge of personality-rights litigation confronting deepfakes and synthetic non-consensual intimate imagery. Situating the doctrinal analysis within National Crime Records Bureau data and international human rights instruments including CEDAW General Recommendation No. 35, the manuscript argues that India's response remains fragmented, reactive, and structurally ill-suited to harms that are borderless, technologically mutable, and disproportionately gendered. Drawing comparative lessons from the United States' TAKE IT DOWN Act, 2025, the United Kingdom's Online Safety Act, 2023, and the European Union's Digital Services Act, it proposes a dedicated statutory framework grounded in consent rather than authenticity, victim-centric takedown mechanisms, gender-neutral drafting, and cross-border cooperation, while cautioning against regulatory overreach that could compromise legitimate expression. It concludes that meaningful protection against digital violence requires a coherent, rights-based legislative response calibrated to an artificial-intelligence-mediated information ecosystem, rather than incremental amendment of instruments never designed for this purpose.

Keywords: digital violence, cyberstalking, deepfakes, non-consensual intimate imagery, Information Technology Act, Bharatiya Nyaya Sanhita, Digital Personal Data Protection Act, online gender-based violence, personality rights

* Author is a Student at Government Law College, Villupuram, Tamil Nadu, India.

** Author is a Student at Government Law College, Chengalpattu, Tamil Nadu, India.

I. INTRODUCTION

The internet, once celebrated as a great equaliser that would democratise voice and access, has also become an instrument of gendered subjugation. What began, in the early 2000s, as isolated instances of obscene messaging and rudimentary cyberstalking has, over two decades, metastasised into a diverse and rapidly evolving ecosystem of harms: cyberstalking, non-consensual dissemination of intimate images, doxxing, sextortion, coordinated online harassment, and, most recently, artificial-intelligence-generated deepfakes that place a woman's face and voice onto sexually explicit or defamatory content without her knowledge or consent. Commentators increasingly use the umbrella term "digital violence against women," or "technology-facilitated gender-based violence," to capture this cluster of harms, recognising that the medium does not diminish the injury; it merely changes its shape, its speed, and its reach.¹

India presents a particularly instructive case study. It combines one of the world's fastest-growing bases of women internet users (even as stark urban-rural and gender divides in digital access persist²) with a criminal-law architecture that has recently undergone wholesale recodification, and a judiciary that has, within the space of three years, moved from adjudicating isolated cyber-obscenity prosecutions to confronting an explosion of deepfake-related litigation, with a reported 375% year-on-year rise in such High Court cases between 2024 and 2025.³ Yet, as this manuscript argues, statutory reform has consistently lagged behind technological harm. The Information Technology Act, 2000 was conceived in an era before smartphones, social media, and generative artificial intelligence; the Bharatiya Nyaya Sanhita, 2023, despite its stated ambition of modernisation, substantially reproduces the architecture of the Indian Penal Code, 1860, with only incremental digital additions; and even the newest instruments, the 2025 and 2026 amendments to the Intermediary Guidelines Rules, arrived only after the harm had already reached crisis proportions.⁴

This manuscript proceeds in nine further parts. Part II conceptualises digital violence against women and offers a working typology of its principal forms. Part III maps the constitutional

¹ See Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1758–66 (2019) (describing the gendered pattern of online abuse and its continuity with offline violence).

² See *Conceptualising Cyber-Crime Against Women: Beyond Numbers and "Online Misbehaviour"*, IMPRI IMPACT & POL'Y RSCH. INST. (Nov. 12, 2025) (citing Nat'l Family Health Survey-5 (2019–21) data showing approximately 33.3% of Indian women aged 15–49 report having ever used the internet, with pronounced urban–rural divergence).

³ *Rethinking Judicial Approaches to Sexually-Explicit Deepfakes: The Case for Article 21-Based Relief Against Nudifying Websites*, TECH L. F., NALSAR UNIV. OF L. (Mar. 26, 2026) (recording a rise from 4 deepfake-related High Court cases in 2024 to 19 in 2025).

⁴ *Id.*

and statutory framework currently governing this terrain in India. Part IV situates the domestic framework within international human rights instruments. Part V traces judicial engagement with digital violence, from early cyber-obscenity jurisprudence to the recent surge of personality-rights and deepfake litigation. Part VI isolates the deepfake phenomenon as a distinct and escalating frontier requiring urgent legislative attention. Part VII situates the analysis within available empirical data, while Part VIII identifies the structural and doctrinal gaps that persist despite recent reform. Part IX draws comparative lessons from the United States, the United Kingdom, and the European Union, and Part X offers recommendations toward a coherent, rights-based statutory response.

II. CONCEPTUALISING DIGITAL VIOLENCE AGAINST WOMEN

A. Definitional Contours

Digital violence against women may be understood as any act of gender-based violence that is committed, facilitated, or amplified through digital technology (computers, mobile devices, the internet, social media platforms, or artificial intelligence tools) and that causes physical, sexual, psychological, social, political, or economic harm to a woman by virtue of her gender. The definition deliberately extends beyond the narrower category of "cybercrime," which is technology-neutral and offence-focused, to capture the gendered pattern of harm: digital violence disproportionately targets women, is frequently sexualised in content, and often functions as an extension of, or precursor to, offline violence, including intimate partner abuse, stalking, and honour-based coercion. The Committee on the Elimination of Discrimination against Women has itself recognised this continuity, observing that gender-based violence occurs across "the redefinition of public and private through technology-mediated environments, such as contemporary forms of violence occurring online and in other digital environments."⁵

Three features distinguish digital violence from its offline analogues and complicate legal response. First, it is characterised by virality and permanence: content that would once have been confined to a single disclosure can be replicated, mirrored, and redistributed across jurisdictions within minutes, such that any single takedown order is almost always under-inclusive. Second, it is frequently anonymous or pseudonymous, permitting perpetrators to evade identification through proxy servers, encrypted applications, or foreign-hosted platforms. Third, and increasingly significant, it is technologically generative: the harm need no longer

⁵ Comm. on the Elimination of Discrimination Against Women, Gen. Recommendation No. 35 on Gender-Based Violence Against Women, Updating Gen. Recommendation No. 19, ¶ 20, U.N. Doc. CEDAW/C/GC/35 (July 14, 2017).

depend on the existence of authentic material at all, since generative artificial intelligence tools can fabricate sexually explicit or defamatory content of a woman who has never been photographed in a compromising situation.⁶

B. A Typology of Digital Violence

The literature and Indian case law together disclose at least seven recurring forms of digital violence against women. Cyberstalking involves the persistent, unwanted monitoring, following, or contacting of a woman through electronic means, including tracking her location, monitoring her social media activity, or repeatedly contacting her despite clear disinterest, conduct now placed on an express statutory footing under Section 78 of the Bharatiya Nyaya Sanhita, 2023.⁷ Online harassment and cyberbullying encompass sustained abusive messaging, threats, and coordinated pile-ons, often amplified by anonymous accounts and bot networks. Non-consensual intimate imagery ("NCII"), colloquially termed "revenge pornography," involves the distribution of sexually explicit images or videos without the subject's consent, whether obtained through a former intimate relationship, hacking, or covert recording amounting to voyeurism.⁸ Doxxing refers to the malicious publication of private identifying information (a home address, a phone number, a workplace) intended to expose a woman to offline harm. Sextortion combines the threat of NCII disclosure with coercive demands for money, further sexual content, or continued relationship. Morphing involves the digital alteration of an authentic photograph to place a woman's face onto explicit or humiliating content. Finally, and most recently, deepfakes use generative adversarial networks and diffusion-based artificial intelligence models to fabricate hyper-realistic sexually explicit or defamatory video, audio, or image content, requiring no authentic underlying material whatsoever.⁹ A related but distinct concern is technology-facilitated intimate partner abuse, in which spyware or "stalkerware" applications are covertly installed on a woman's device by a partner or ex-partner to monitor her calls, messages, and location in real time, a form of digital coercive control that frequently escapes the categories used in official crime statistics.

III. CONSTITUTIONAL AND STATUTORY FRAMEWORK IN INDIA

A. Constitutional Anchors

⁶ See Citron & Chesney, *supra* note 1, at 1772–78.

⁷ The Bharatiya Nyaya Sanhita, No. 45 of 2023, § 78, INDIA CODE (2023).

⁸ The Bharatiya Nyaya Sanhita, No. 45 of 2023, § 77, INDIA CODE (2023); see also *Cyber Harassment on Women*, DRISHTI JUDICIARY (2025).

⁹ See *Deepfakes and Dignity: Why Indian Laws Need Reform Against Non-Consensual AI-Generated Content Beyond Section 67A*, LEGAL J. ON TECH. (Apr. 6, 2026).

India possesses no free-standing constitutional guarantee against digital violence, but the Supreme Court's recognition of privacy as a fundamental right under Article 21 in *Justice K.S. Puttaswamy (Retd.) v. Union of India* provides the doctrinal foundation upon which statutory and judicial responses are increasingly built.¹⁰ The Court held that informational privacy (the ability to control the dissemination of one's own image, likeness, and personal data) is an inseverable facet of the right to life and personal liberty, and that any State restriction upon it must satisfy the tripartite test of legality, legitimate aim, and proportionality.¹¹ This reasoning has since migrated into digital violence jurisprudence: Delhi High Court decisions granting takedown relief against non-consensual intimate content and deepfakes routinely invoke *Puttaswamy* to ground a woman's entitlement to control her own image, independent of whether she is a public figure entitled to protect commercially valuable personality rights.

B. The Information Technology Act, 2000

The Information Technology Act, 2000 remains the primary special statute addressing cyber-harms, though it was not drafted with gendered digital violence specifically in contemplation. Section 66E penalises the capturing, publishing, or transmission of images of a person's private area without consent, and is the principal provision invoked in voyeurism and NCII prosecutions.¹² Sections 67 and 67A criminalise the publication or transmission of obscene and sexually explicit material respectively, with escalating penalties (up to three years' imprisonment and a five-lakh-rupee fine for a first conviction under Section 67, and up to five years and ten lakh rupees under Section 67A), while Section 67B specifically addresses child sexual abuse material.¹³ Sections 66C and 66D, dealing respectively with identity theft and cheating by personation using a computer resource, have assumed unanticipated importance in the deepfake context: commentators have read the phrase "unique identification feature" in Section 66C to encompass facial geometry and voice biometrics, rendering the non-consensual creation of a deepfake bearing a woman's likeness a form of statutory identity theft.¹⁴ Section 72 penalises breach of confidentiality and privacy by persons who secure access to electronic material in the exercise of powers under the Act, while Section 79 confers conditional safe harbour upon intermediaries, contingent upon compliance with due diligence obligations prescribed under the Intermediary Guidelines Rules.

¹⁰ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

¹¹ *Id.* at ¶¶ 310, 325 (*K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2019) 1 S.C.C. 1) (elaborating the proportionality standard).

¹² Information Technology Act, No. 21 of 2000, § 66E, INDIA CODE (2000).

¹³ Information Technology Act, No. 21 of 2000, §§ 67, 67A, 67B, INDIA CODE (2000).

¹⁴ See *Deepfake Liability in India: AI Legal Guide*, AHLAWAT & ASSOCS. (Apr. 27, 2026).

C. The Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 ("BNS"), which replaced the Indian Penal Code, 1860 with effect from 1 July 2024, substantially retained the architecture of the erstwhile Sections 354A to 354D and 509 while renumbering them. Section 75 (previously Section 354A) addresses sexual harassment; Section 76 (previously 354B) addresses assault or use of criminal force with intent to disrobe; Section 77 (previously 354C) addresses voyeurism, including the non-consensual capture and dissemination of images of a woman engaged in a private act; Section 78 (previously 354D) addresses stalking and, significantly, expressly extends to the monitoring of a woman's use of the internet, email, or electronic communication, thereby placing cyberstalking on an express statutory footing; and Section 79 (previously Section 509) addresses words, gestures, or acts intended to insult the modesty of a woman.¹⁵ Section 78 further recognises statutory exceptions where the monitoring is undertaken for *bona fide* crime prevention or pursuant to legal authority. Sections 111 and 212 of the BNS, dealing respectively with organised crime and furnishing false information, have been read to extend to coordinated deepfake campaigns and synthetic disinformation, offering an additional, if indirect, layer of criminal accountability.¹⁶ Notwithstanding these advances, the BNS continues to define the offences of sexual harassment and stalking in gender-specific terms, restricting the perpetrator to "any man," a structural limitation that the Justice J.S. Verma Committee had recommended be corrected as early as 2013, and one that sits uneasily with the increasingly gender-diverse landscape of digital harassment.¹⁷

D. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ("DPDP Act") introduces, for the first time in Indian law, a comprehensive consent-based framework for the processing of personal data, and carries direct if underexplored relevance to digital violence. Section 6 requires that consent for processing personal data be free, specific, informed, unconditional, and unambiguous, communicated through clear affirmative action.¹⁸ Where a perpetrator scrapes a woman's publicly available photographs to train a generative model or to produce a deepfake, the resulting processing of her biometric and facial data occurs without any of the safeguards

¹⁵ The Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 75–79, INDIA CODE (2023); *see also* BUREAU OF POLICE RSCH. & DEV., *Comparison Summary: BNS to IPC* (2024).

¹⁶ *See Deepfake Regulation India 2025: MeitY's Comprehensive IT Rules Amendment*, KHURANA & KHURANA / MONDAQ (Dec. 16, 2025) (citing The Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 111, 212, INDIA CODE (2023)).

¹⁷ JUSTICE J.S. VERMA, REPORT OF THE COMM. ON AMENDMENTS TO CRIM. L. 128–30 (Jan. 23, 2013); *see also Criminal Law Bills 2023 Decoded #2: Concerns with the Proposed Landscape of Sexual Offences in BNS 2023*, P39A CRIM. L. BLOG (Oct. 11, 2023).

¹⁸ The Digital Personal Data Protection Act, No. 22 of 2023, § 6, INDIA CODE (2023).

contemplated by Section 6, arguably constituting an independent statutory violation quite apart from any prosecution under the IT Act or BNS. The DPDP Act's penalty structure (financial penalties of up to two hundred and fifty crore rupees for significant breaches) is considerably more severe than anything available under the IT Act, and offers, at least in principle, a potent deterrent against platforms and data fiduciaries that fail to prevent unauthorised biometric harvesting.¹⁹ However, the DPDP Act's enforcement architecture is administered by the Data Protection Board rather than criminal courts, and its interplay with the IT Act and BNS (including questions of concurrent jurisdiction, victim standing, and compensation) remains, as of this writing, substantially untested.

E. The Intermediary Guidelines Rules, 2021 and Its 2025–2026 Amendments

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due diligence obligations on intermediaries as a precondition for the safe harbour under Section 79 of the IT Act, including obligations to act upon actual knowledge of unlawful content and to remove non-consensual intimate imagery within a specified window upon complaint.²⁰ The Rules were substantially amended twice in quick succession to address the specific challenge of synthetically generated content. The 2025 amendment, in force from 15 November 2025, introduced the concept of "synthetically generated information," requiring significant social media intermediaries to prompt users to declare AI-generated uploads, deploy automated verification tools, and display a clear disclaimer where content is confirmed synthetic; critically, it dispensed with the earlier requirement that removal of unlawful synthetic content await a court order or government notification, instead obliging platforms to act on "reasonable efforts."²¹ The February 2026 amendment went further still, compressing the takedown window for government- or court-flagged synthetic content to three hours, and non-consensual intimate imagery specifically to two hours, while introducing labelling, metadata-traceability, and quarterly-warning obligations.²² Non-compliance carries the risk of losing safe harbour altogether, exposing platforms (and, under Section 85 of the IT Act, their compliance officers personally) to direct liability.²³

¹⁹ See *Deepfake Regulation India 2025*, *supra* note 16 (citing The Digital Personal Data Protection Act, No. 22 of 2023, sched. (2023)).

²⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India).

²¹ *India Tightens Rules on Deepfakes and AI-Generated Content*, LAW.ASIA (Feb. 10, 2026).

²² *IT Rules 2026 Deepfake Regulation: Three Hour Takedowns and AI Labelling Obligations*, MONDAQ (Mar. 18, 2026).

²³ See *Deepfake Liability in India*, *supra* note 14 (discussing Information Technology Act, No. 21 of 2000, § 85, INDIA CODE (2000)).

These amendments represent a marked shift from a reactive, court-order-dependent takedown model to a proactive, platform-administered compliance regime. Yet the shift is not without constitutional risk. Commentators have argued that compressed takedown timelines, undefined verification thresholds, and the absence of individualised assessment sit uneasily with the proportionality standard articulated in *Puttaswamy* and with the anti-prior-restraint principle underlying *Shreya Singhal v. Union of India*, which held that intermediaries could not be compelled to proactively monitor content absent a court or government order.²⁴ The tension between speed of redress (essential given the virality of NCII and deepfake content) and the risk of converting platforms into arbiters of truth and authenticity is, at present, unresolved.

IV. INTERNATIONAL LEGAL INSTRUMENTS AND STANDARDS

India's obligations under international human rights law, though not directly enforceable absent domestic incorporation, inform the interpretive backdrop against which its statutory framework must be assessed. The Committee on the Elimination of Discrimination against Women, in General Recommendation No. 35 of 2017 (updating the foundational General Recommendation No. 19 of 1992) expressly recognised technology-mediated environments as a site of contemporary gender-based violence, and identified "the ideology of men's entitlement and privilege over women" and the "need to assert male control or power" as structural drivers that persist, and indeed find new expression, in digital spaces.²⁵ General Recommendation No. 35 calls upon States parties to ensure that legal frameworks address the "continuum of violence" experienced by women across offline and online contexts, rather than treating digital harms as a discrete, lesser category of offence.²⁶

India is also a party to the Convention on the Elimination of All Forms of Discrimination against Women, 1979, which, through Article 1's definition of discrimination and the Committee's subsequent jurisprudence, has been read to encompass the State's due-diligence obligation to prevent, investigate, and remedy gender-based violence perpetrated by private actors, including through digital means. While CEDAW itself creates no directly enforceable domestic right absent legislative incorporation consistent with the dualist orientation reflected in decisions such as *Vishaka v. State of Rajasthan*, its General Recommendations have repeatedly been invoked by Indian courts as an interpretive aid in construing the scope of statutory and

²⁴ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India); see also *India's New IT Rules on Deepfakes Threaten to Entrench Online Censorship*, TECH POL'Y PRESS (Nov. 7, 2025).

²⁵ CEDAW Gen. Recommendation No. 35, *supra* note 5, ¶ 19.

²⁶ *Id.* ¶¶ 10, 20.

constitutional protections for women, and offer a useful benchmark against which the adequacy of India's fragmented digital violence framework may be measured.

V. JUDICIAL RESPONSES

A. Early Cyber Jurisprudence

India's first reported conviction for a cyber-offence against a woman, *State of Tamil Nadu v. Suhas Katti*, concerned the posting of obscene, defamatory messages about a woman in an online messaging group, along with the circulation of her contact details inviting harassment; the accused was convicted under the modesty and defamation provisions of the Indian Penal Code, 1860 read with Section 67 of the IT Act.²⁷ The case, decided within seven months of the complaint being filed, is frequently cited as a rare instance of expeditious cyber-justice, but it also illustrates the limited doctrinal toolkit then available: reliance on general obscenity and modesty provisions never designed for networked harm. A decade later, in *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act, which had criminalised sending "grossly offensive" or "menacing" information through a computer resource, as unconstitutionally vague and violative of the freedom of speech guaranteed under Article 19(1)(a).²⁸ While *Shreya Singhal* is celebrated as a free-speech landmark, its practical effect was to remove a provision that, however imperfectly, had been invoked in a subset of online harassment cases, leaving the field to be filled by Sections 66E, 67, and 67A of the IT Act and the modesty and stalking provisions of the erstwhile IPC, now reproduced in the BNS.

B. Personality Rights and Deepfake Litigation

The most significant recent judicial development lies in the surge of personality-rights litigation before the Delhi and Bombay High Courts. In *Anil Kapoor v. Simply Life India*, the Delhi High Court granted an omnibus, *ex parte* injunction restraining the unauthorised use of the actor's name, image, voice, and persona (including through artificial intelligence tools, GIFs, and AI-generated content), recognising that technological misappropriation of one's likeness could cause both commercial and dignitary harm.²⁹ In *Arijit Singh v. Codible Ventures LLP*, the Bombay High Court similarly restrained the unauthorised AI-based cloning of a performer's vocal attributes, characterising such misuse as an infringement of personality, publicity, and moral rights under the Copyright Act, 1957, and observing that the ease with which performers could now be commercially exploited by artificial intelligence "shocked the conscience" of the

²⁷ *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004 (Ct. of Metropolitan Magistrate, Egmore, Nov. 5, 2004) (India).

²⁸ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1, ¶¶ 76–83 (India).

²⁹ *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914 (India).

court.³⁰ More recently, in *Sadhguru Jagadish Vasudev v. Igor Isakov*, the Delhi High Court introduced what commentators have termed a "dynamic+" injunction, extending protection prospectively to future, as-yet-unidentified instances of AI-generated misuse, rather than confining relief to specifically identified infringing content.³¹

Crucially, this jurisprudence has not remained confined to celebrities. In *Kamya Buch v. JIX5A*, the Delhi High Court granted *ad interim* relief to a non-celebrity claimant whose morphed, sexually explicit images had been disseminated online, directing multiple platforms to take down the offending content to protect her privacy and dignity.³² Similarly, in *Ankur Warikoo v. John Doe*, a social media influencer obtained a "John Doe" injunctive order restraining all unidentified entities from using his name, image, voice, and likeness (including through artificial intelligence or deepfake technology) for personal or commercial gain, illustrating courts' growing willingness to grant prospective, defendant-agnostic relief in the face of anonymous online misuse.³³ Empirical mapping of deepfake litigation before Indian High Courts between 2023 and 2025 reveals, however, a stark asymmetry: women constitute only a small minority of petitioners seeking takedown relief, notwithstanding that they are disproportionately the targets of sexually explicit synthetic content, a pattern attributable to the litigation costs, reputational exposure, and access-to-justice barriers that disproportionately burden ordinary women relative to well-resourced public figures.³⁴

C. Toward an Article 21-Based Approach

A significant doctrinal debate has emerged over the appropriate juridical basis for deepfake and NCII takedown relief. Much of the existing case law grounds relief in personality and publicity rights, doctrines historically developed to protect the commercial value of a celebrity's persona, which risks limiting the precedential reach of favourable rulings to those who already possess the economic and reputational capital to litigate.³⁵ An emerging body of academic commentary argues that courts should instead ground takedown relief squarely in the right to privacy and dignity under Article 21, following the logic of *Puttaswamy* and the earlier decision in *R. Rajagopal v. State of Tamil Nadu* recognising a right to control the dissemination of one's image

³⁰ *Arijit Singh v. Codible Ventures LLP*, 2024 SCC OnLine Bom 2445 (India); see *Deepfake Liability in India*, *supra* note 14.

³¹ *Sadhguru Jagadish Vasudev v. Igor Isakov*, CS (COMM) 578/2025 (Del. H.C. May 30, 2025) (India); see also *Deepfake Regulation India 2025*, *supra* note 16.

³² *Kamya Buch v. JIX5A* (Del. H.C.) (India); see *Me, Myself and AI: Chasing Deepfakes Across Borders Without Losing Your Rights*, SCC OnLine BLOG (Nov. 8, 2025).

³³ *Ankur Warikoo v. John Doe* (Del. H.C.) (India); see SCC OnLine BLOG, *supra* note 32.

³⁴ *Rethinking Judicial Approaches to Sexually-Explicit Deepfakes*, *supra* note 3.

³⁵ *Id.*

and personal narrative.³⁶ Such a reorientation would make the remedy accessible to the ordinary woman victimised by NCII or a deepfake, regardless of whether she possesses any commercially exploitable persona, and would better align India's judicial response with the gendered reality of digital violence, where the overwhelming majority of victims are private individuals rather than public figures.

VI. THE DEEFAKE DILEMMA: A NEW FRONTIER OF DIGITAL VIOLENCE

Deepfake technology represents a qualitative, not merely incremental, escalation of digital violence against women. Unlike traditional NCII, which requires the prior existence of an authentic image or video, generative adversarial networks and diffusion models can fabricate convincing sexually explicit or defamatory content of a woman entirely from publicly available photographs; a school or workplace profile picture is, in principle, sufficient raw material.³⁷ The 2023 viral deepfake video misappropriating the likeness of actor Rashmika Mandanna, which prompted the Prime Minister to describe the phenomenon as a national crisis, marked a turning point in public and legislative attention, though the underlying harm had already been escalating for ordinary, non-celebrity women for some time.³⁸

India's response to date exposes an important conceptual confusion. Much existing doctrine treats sexually explicit deepfakes as a species of "obscenity" prosecutable under Section 67A of the IT Act or Section 294 of the BNS; defence counsel have accordingly sought to characterise synthetic content as protected "artistic fantasy" rather than exploitative material, since no actual human activity underlies the depiction.³⁹ This framing, it is argued, misidentifies the gravamen of the harm: the wrong lies not in the content's obscenity but in the absence of the depicted woman's consent to being represented at all, a violation of dignity and autonomy rather than of public morality.⁴⁰ Framing deepfakes as obscenity offences therefore risks under-inclusiveness, permitting technically "non-obscene" but still non-consensual and humiliating synthetic content to escape sanction, and doctrinal instability, inviting speech-protective defences unavailable where the true harm is consent-based rather than morality-based.

The 2025 and 2026 amendments to the Intermediary Guidelines Rules represent the first sustained legislative attempt to grapple with this distinct harm, introducing the regulatory category of "prohibited synthetically generated information," encompassing non-consensual

³⁶ *R. Rajagopal v. State of T.N.*, (1994) 6 S.C.C. 632 (India); see also SCC ONLINE BLOG, *supra* note 32.

³⁷ See Citron & Chesney, *supra* note 1, at 1758–60.

³⁸ *India Tightens Rules on Deepfakes*, *supra* note 21.

³⁹ *Deepfakes and Dignity*, *supra* note 9 (discussing The Bharatiya Nyaya Sanhita, No. 45 of 2023, § 294, INDIA CODE (2023)).

⁴⁰ *Id.*

intimate imagery, impersonation and fraud-oriented deepfakes, and deceptive political content, alongside compressed takedown timelines and mandatory labelling.⁴¹ Yet the amendments operate through subordinate legislation under the IT Act rather than a dedicated statute, leaving unresolved foundational questions: the standard of liability applicable to the developers of "nudifying" applications used to generate NCII, the availability of statutory compensation for victims, and the treatment of purely private, unpublished synthetic content that nonetheless causes psychological harm through the mere threat of disclosure.⁴²

VII. THE EMPIRICAL DIMENSION: DATA AND THE REPORTING GAP

The National Crime Records Bureau's *Crime in India* series offers the principal administrative window into the scale of digital violence in India, though its categories remain ill-suited to capturing gendered cyber-harm with precision. The 2023 report recorded 86,420 cybercrime cases nationally, a 31.2% increase over 2022, with the cybercrime rate rising from 4.8 to 6.2 cases per lakh population; the 2024 report recorded a further increase to 101,928 cases, a rate of 7.3 per lakh population.⁴³ Crimes against women overall stood at 448,211 cases in 2023, marginally declining to approximately 441,000 cases in 2024, a figure that must be read cautiously, since a decline in registered cases need not indicate a genuine reduction in underlying harm and may instead reflect under-reporting, victim distrust of the criminal justice process, or continuing misclassification of gendered cyber-harm under generic headings such as "obscenity" or "insult to modesty" rather than as a distinct, technology-facilitated offence.⁴⁴

The gap is compounded by persistent digital access asymmetries: only around a third of Indian women report having ever used the internet, with sharp urban-rural divergence, meaning official cybercrime statistics likely undercount harm experienced by women with limited digital literacy, who may simultaneously be more vulnerable to covert surveillance and image-based abuse by intimate partners, and less equipped to detect or report such abuse in the first place.⁴⁵ These data limitations counsel caution against relying solely on registered-case statistics to gauge the adequacy of legal reform, and instead support the doctrinal and structural analysis undertaken in this manuscript.

⁴¹ *IT Rules 2026 Deepfake Regulation*, *supra* note 22.

⁴² *Deepfakes and Dignity*, *supra* note 9.

⁴³ *NCRB 2023 Report: Rise in Crimes Against Women, Cybercrime, Farmer Suicides*, NAT'L HERALD INDIA (Sept. 30, 2025); *Crime in India 2024: NCRB Report Highlights Emerging Security and Social Challenges*, RAU'S IAS (2026).

⁴⁴ RAU'S IAS, *supra* note 43; IMPRI IMPACT & POL'Y RSCH. INST., *supra* note 2.

⁴⁵ IMPRI IMPACT & POL'Y RSCH. INST., *supra* note 2.

VIII. STRUCTURAL AND DOCTRINAL GAPS

A. The Absence of a Dedicated Legislative Framework

Perhaps the most fundamental gap in India's response to digital violence against women is the absence of any dedicated statute. Protection is instead assembled from provisions scattered across the IT Act, the BNS, the DPDP Act, and subordinate rules, each drafted with a different primary purpose (the IT Act as a general cyber-law and e-commerce facilitation statute, the BNS as a general penal code, and the DPDP Act as a data-protection instrument), none conceived specifically to address the gendered, technologically mutable, and rapidly evolving nature of digital violence.⁴⁶ This fragmentation produces both interpretive uncertainty as to which provision governs a given fact pattern, and enforcement gaps, since victims and even investigating officers may be uncertain which statute, and which police cell, has primary jurisdiction.

B. Jurisdictional and Cross-Border Enforcement Challenges

Digital violence routinely transcends territorial boundaries: content may be uploaded from a server outside India, hosted by a foreign platform, and viewed by an Indian victim, raising acute questions of jurisdiction, applicable law, and enforceability of Indian court orders against foreign-domiciled respondents.⁴⁷ While Indian courts have increasingly granted "John Doe" orders restraining unidentified defendants and directing intermediaries to act against future infringing uploads, the practical efficacy of such orders against platforms with no assets or presence in India remains limited, and India lacks a functioning mutual legal assistance framework for the expedited cross-border removal of NCII comparable to those under discussion in other jurisdictions.

C. Evidentiary and Procedural Hurdles

Victims of digital violence face acute evidentiary burdens: establishing the authenticity of screenshots, preserving metadata before platform-side deletion, and, in the deepfake context, proving that content is synthetic in the first place, a determination that increasingly requires specialised forensic expertise unavailable to under-resourced state cyber cells. The absence of a uniform chain-of-custody protocol for digital evidence across states, combined with the reluctance of many police stations to register complaints under the correct provision rather than

⁴⁶ See *Deepfakes and Indian Law: Legal Framework, Privacy, Cybercrime, AI Regulation & Supreme Court Analysis*, LEGAL SERV. INDIA (June 27, 2026) (noting the absence of a dedicated deepfake or digital-violence statute in India).

⁴⁷ See SCC ONLINE BLOG, *supra* note 32.

a generic "obscenity" or "defamation" heading, continues to produce systemic under-prosecution.⁴⁸

D. Access to Justice Barriers

Finally, the emerging deepfake jurisprudence itself reveals an uncomfortable class and gender skew: it is overwhelmingly public figures and celebrities (possessed of the resources, legal counsel, and reputational stakes to pursue urgent injunctive relief) who have successfully obtained takedown orders, while ordinary women, who constitute the overwhelming majority of victims of image-based sexual abuse, remain acutely underrepresented in the reported case law.⁴⁹ A rights-based reorientation of the remedy, discussed in Part V.C above, alongside accessible, low-cost grievance redressal mechanisms such as strengthened state Cyber Crime Cells and the national Cyber Crime Reporting Portal, is necessary to correct this imbalance.

IX. COMPARATIVE PERSPECTIVES

A. United States: The TAKE IT DOWN Act, 2025

The United States' Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, enacted in May 2025, criminalises the intentional publication of non-consensual intimate visual depictions (whether authentic or AI-generated "digital forgeries") where there is intent to cause harm or actual harm results, while embedding express exceptions for education, satire, journalism, and matters of public concern.⁵⁰ Its narrowly tailored, intent-based approach, applicable uniformly to both real and synthetic imagery, offers a template that avoids some of the overbreadth concerns raised against India's more platform-centric, takedown-driven model, since liability turns on the perpetrator's consent violation rather than on a downstream platform's speed of removal alone.

B. United Kingdom: The Online Safety Act, 2023

The United Kingdom's Online Safety Act, 2023 imposes statutory duties of care on platforms to proactively identify and remove illegal content, including intimate image abuse, and separately criminalises the non-consensual sharing, and, following subsequent reform, the creation of intimate images, without requiring proof that the perpetrator intended to cause distress to the victim, a lower threshold than that historically required under English law and

⁴⁸ See LEGAL SERV. INDIA, *supra* note 46.

⁴⁹ *Rethinking Judicial Approaches to Sexually-Explicit Deepfakes*, *supra* note 3.

⁵⁰ Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act) (2025); see *India's New IT Rules on Deepfakes*, *supra* note 24.

one that better reflects the reality that much NCII is shared for peer validation or financial gain rather than out of malice toward the specific victim.

C. European Union: The Digital Services Act

The European Union's Digital Services Act imposes graduated due-diligence and risk-assessment obligations on online platforms calibrated to their size and systemic influence, requiring very large platforms to conduct regular risk assessments addressing gender-based violence and to provide accessible, victim-centred notice-and-action mechanisms, backed by the possibility of substantial turnover-based fines for systemic non-compliance.⁵¹ Unlike India's rules-based approach, the Digital Services Act is anchored in a directly applicable regulation subject to full legislative and judicial oversight rather than executive rule-making, lending it greater democratic legitimacy and doctrinal stability.

Taken together, these frameworks suggest two lessons for Indian reform. First, the choice between real and synthetic imagery should not determine the availability of legal protection, since the injury to dignity and autonomy is substantively identical regardless of the technical means by which the content was produced. Second, platform accountability is best anchored in primary legislation subject to full legislative and judicial scrutiny, rather than delegated rule-making that risks both under-inclusiveness in protection and constitutional vulnerability on grounds of proportionality and prior restraint.

X. RECOMMENDATIONS

First, India requires a dedicated statute on technology-facilitated gender-based violence, consolidating and clarifying the presently scattered provisions of the IT Act, BNS, and DPDP Act, and expressly extending liability to the creation, and not merely the dissemination, of non-consensual synthetic sexual content, irrespective of whether the underlying depiction is authentic.⁵² Second, the offences of stalking and sexual harassment under Sections 75 and 78 of the BNS should be rendered gender-neutral in their application, consistent with the 2013 Verma Committee recommendation, without diminishing the enhanced protections presently available to women. Third, courts should consistently ground deepfake and NCII takedown relief in the right to privacy and dignity under Article 21, rather than exclusively in personality and publicity rights, to ensure that non-celebrity victims enjoy equal access to expedited remedies. Fourth, Parliament should establish a statutory victim compensation scheme, potentially funded through

⁵¹ Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1.

⁵² See LEGAL SERV. INDIA, *supra* note 46 (recommending a dedicated statute, mandatory labelling, fast-track removal procedures, and victim compensation).

penalties recovered under the DPDP Act and the Intermediary Guidelines Rules, to address the psychological, reputational, and economic harm suffered by victims independent of the outcome of criminal prosecution.

Fifth, capacity-building of state Cyber Crime Cells, including dedicated digital forensic units capable of authenticating synthetic media, is essential to translate statutory protection into enforceable reality. Sixth, India should pursue bilateral and multilateral mutual legal assistance arrangements specifically calibrated to the expedited cross-border removal of NCII and deepfake content, given the demonstrated inadequacy of purely domestic injunctive relief against foreign-hosted platforms. Finally, any further tightening of intermediary takedown obligations must be accompanied by clear, judicially reviewable standards for synthetic-content verification, to avoid the proportionality and prior-restraint concerns identified in Part III.E, ensuring that the pursuit of victim protection does not come at the cost of legitimate expression.

XI. CONCLUSION

Digital violence against women sits at the uneasy intersection of constitutional privacy doctrine, cyber law, and an artificial intelligence ecosystem evolving considerably faster than Parliament's capacity to legislate. India's statutory response (assembled piecemeal across the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and successive amendments to the Intermediary Guidelines Rules) has undeniably expanded in scope and urgency, particularly in its recent turn toward regulating synthetically generated content. Yet the underlying architecture remains reactive rather than anticipatory, fragmented rather than coherent, and, notwithstanding an encouraging body of judicial innovation, disproportionately accessible to the well-resourced rather than to the ordinary woman who constitutes the true face of this harm. A durable response demands not merely further amendment of existing instruments but a dedicated, rights-based statutory framework: one that treats consent, not authenticity, as the touchstone of liability, and that is calibrated to a digital ecosystem in which the line between the real and the synthetic has, for the purposes of dignity and harm, effectively ceased to matter.
