ISSN: 2583-7354

International Journal of Emerging Knowledge Studies

Publisher's Home Page: https://www.ijeks.com/

Fully Open Access Research Paper

Artificial Intelligence-Generated Deepfake Crimes Against Women in India: Evaluating the Adequacy of the Existing Legal Framework and the Need for Legal Reforms

Nadeem Alam[1*] Shakeel Ahmad[2]

[1]Research Scholar, Department of Political Science, Aligarh Muslim University, Aligarh, India.

[2]Professor & Dean, Faculty of Law, Aligarh Muslim University, Aligarh, India.

DOI: https://doi.org/10.70333/ijeks-05-07-002

*Corresponding Author: alam.nadeem94@gmail.com

Article Info: - Received : 19 May 2026 **Accepted** : 25 June 2026 **Published** : 30 June 2026

Abstract

The proliferation of artificial intelligence (AI)-generated deepfakes has created a distinctly gendered form of technology-facilitated abuse: empirical audits consistently find that most deepfake content online is pornographic and that its subjects are almost exclusively women. India has no dedicated parliamentary statute on deepfakes; victims must instead invoke a mosaic of technology-neutral provisions under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the constitutional guarantees of privacy and dignity recognised in Justice K.S. Puttaswamy v. Union of India (2017). Employing doctrinal legal research grounded in feminist legal theory and informational privacy, and relying exclusively on verifiable secondary sources, this article evaluates whether that framework adequately regulates deepfake crimes against women. The analysis incorporates the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified vide G.S.R. 120(E) dated 10 February 2026, which introduced the regulatory category of "synthetically generated information", mandatory labelling and provenance metadata, and takedown timelines of two to three hours. The article finds that although the 2026 amendments significantly advance platform accountability, the framework remains structurally reactive: it contains no offence of creating or distributing non-consensual synthetic intimate imagery, provides no statutory compensation for victims, and confronts persistent evidentiary, forensic, and jurisdictional obstacles. Drawing on comparative developments in the European Union, the United Kingdom, the United States, and Australia, the article proposes a prioritised reform agenda—immediate criminalisation, medium-term victim-centred remedies and a dedicated regulator, and long-term forensic and governance measures—drafted within the free-speech discipline of Shreya Singhal v. Union of India (2015).

Keywords: *Deepfakes, Artificial Intelligence, Image-Based Sexual Abuse, Non-Consensual Intimate Imagery, Information Technology Act, Bharatiya Nyaya Sanhita, Synthetically Generated Information, Women's Rights, Privacy, Platform Liability.*

ISSN: 2583-7354

1. Introduction

Deepfake technology sits at the intersection of two of the most consequential developments of the digital age: the democratisation of generative artificial intelligence and the persistence of gender-based violence in online spaces. A deepfake is synthetic audio-visual media in which a person's face, body, or voice is digitally fabricated or substituted using deep-learning techniques so convincingly that the output is difficult to distinguish from authentic recordings **(Chesney & Citron, 2019; Mirsky & Lee, 2021)**. What began as a niche research capability has become widely accessible through consumer-grade applications, and its most prevalent documented real-world use has not been satire or cinema but sexual abuse. The first systematic audit of the deepfake ecosystem found that 96% of deepfake videos then online were pornographic and that the subjects of the leading deepfake pornography websites were exclusively women **(Ajder et al., 2019)**; a ten-country survey in 2024 confirmed both the growing prevalence of non-consensual synthetic intimate imagery and widespread public ignorance of its illegality **(Umbach et al., 2024)**. Deepfake abuse is therefore not a gender-neutral phenomenon incidentally affecting women; it is a form of image-based sexual abuse that reproduces, in algorithmic form, older patterns of sexual objectification, harassment, and silencing of women **(McGlynn & Rackley, 2017)**.

India presents an acute site for this inquiry. It has one of the world's largest bases of internet users, a rapidly expanding generative-AI ecosystem, and a documented rise in registered cybercrime, from 50,035 cases in 2020 to 86,420 cases in 2023 **(NCRB, 2022, 2023, 2025)**. High-profile incidents in late 2023 involving morphed videos of Indian film actresses brought deepfakes to the centre of national policy attention, prompting advisories from the Ministry of Electronics and Information Technology (MeitY) in November and December 2023 directing intermediaries to comply with existing due-diligence obligations concerning impersonation and morphed imagery **(MeitY, 2023)**. Public interest litigation before the Delhi High Court, including *Chaitanya Rohilla v. Union of India* and *Rajat Sharma v. Union of India*, pressed the Union Government to regulate deepfakes, and in November 2024 the Court recorded the constitution of a MeitY committee to examine the issue. The regulatory trajectory culminated, for the present, in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified vide Gazette notification G.S.R. 120(E) dated 10 February 2026 and in force from 20 February 2026, which introduced into Indian law a definition of "synthetically generated information" (SGI) and an associated due-diligence regime **(MeitY, 2026a)**.

A terminological clarification frames the entire analysis. When this article states that India has "no deepfake law", the claim is that no Act of Parliament defines or criminalises deepfake abuse as such; when it states that SGI has been "introduced into Indian law", the reference is to subordinate legislation—rules framed by the executive under Section 87 of the Information Technology Act, 2000. The distinction is not pedantic. Subordinate legislation binds intermediaries but cannot create offences against perpetrators, is confined by the rule-making power of the parent Act, and can be amended without parliamentary deliberation. India therefore regulates the platforms that carry deepfakes without punishing, compensating for, or even naming the underlying wrong. Whether that architecture is adequate for women victims is the question this article pursues, and it does so through a defined theoretical lens, a doctrinal method, and a comparative benchmark of jurisdictions that legislated directly on synthetic intimate imagery between 2023 and 2025.

2. Theoretical Framework

The analysis proceeds from two complementary theoretical positions. The first is feminist legal theory as applied to technology-facilitated abuse. Feminist scholarship

reconceptualised the non-consensual creation and distribution of sexual imagery not as an obscenity or public-morality problem but as sexual abuse—a violation of sexual autonomy located on a continuum with other forms of sexual violence **(McGlynn & Rackley, 2017; McGlynn, Rackley, & Houghton, 2017)**. Citron's concept of "sexual privacy" sharpens the point: control over the boundaries of one's intimate life, including its representation, is foundational to equality and to participation in public life, and its invasion operates as a mechanism of gendered subordination **(Citron, 2019; Citron & Franks, 2014)**. On this account, the legal test of adequacy is whether the law names the wrong as a consent violation, centres the victim's remedial position, and addresses the structural (not merely individual) character of the harm.

The second position is the theory of informational privacy and its constitutional articulation. Westin's classical definition of privacy as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others **(Westin, 1967)** anticipates the deepfake problem with precision: synthesis from harvested images is an extreme negation of informational self-determination, because the subject loses control not only over true information but over fabricated information credibly attributed to her. In Indian constitutional law this theory is domesticated by **Puttaswamy (2017)**, which recognised informational privacy and decisional autonomy as facets of Article 21. The scholarship on digital constitutionalism supplies the final element: as private platforms become the effective adjudicators of online rights, constitutional values must be translated into the regulatory design governing those platforms, rather than confined to vertical state-citizen relations **(De Gregorio, 2021)**. Together, these lenses generate the evaluative criteria applied throughout: (i) is the wrong correctly characterised (consent, not obscenity); (ii) is the victim's remedy effective and accessible; (iii) is platform power constitutionally disciplined; and (iv) is the regime proportionate to expressive freedoms.

3. Literature Review

3.1. Foundational Legal Scholarship

The foundational legal analysis is **Chesney and Citron's (2019)** study, which mapped deepfake threats to privacy, democracy, and national security and identified the structural mismatch between fabricated-but-realistic depictions and doctrines—privacy torts, defamation, obscenity—built around authentic material. Their further insight, the "liar's dividend", predicts a systemic evidentiary externality: as fabrication becomes plausible, authentic recordings become deniable. Earlier, **Citron and Franks (2014)** made the canonical case for criminalising non-consensual pornography, arguing that civil remedies systematically fail victims confronting anonymous or judgment-proof perpetrators. **Gieseke (2020)** extended the critique specifically to deepfake pornography, demonstrating that United States tort and criminal law, as it then stood, could not reach purely synthetic depictions.

3.2. Conceptual and Empirical Scholarship on Image-Based Sexual Abuse

McGlynn and Rackley (2017) developed the framework of "image-based sexual abuse" to replace the victim-blaming and under-inclusive label of "revenge porn", expressly encompassing fabricated imagery; **McGlynn, Rackley, and Houghton (2017)** documented empirically that victims experience such abuse as a violation comparable to physical sexual offences. **Henry and Powell (2018)** situated these harms within the broader category of technology-facilitated sexual violence and identified persistent under-reporting. Empirically, **Ajder et al. (2019)** provided the first quantitative audit of the deepfake ecosystem; **Flynn, Powell, Scott, and Cama (2022)** supplied multi-country survey evidence that digitally altered imagery abuse is prevalent and gendered; and **Umbach, Henry, Beard, and Berryessa (2024)** confirmed, across ten countries, both rising exposure to synthetic NCII and low public awareness of its wrongfulness. On the perpetration side, **Maddocks (2020)** showed continuity between pornographic and "political" deepfakes as instruments for silencing women, while **Öhman (2020)** and **Viola and Voto (2023)** interrogated the claim that private creation

without distribution is harmless, concluding that creation itself violates the depicted person's standing as an autonomous subject.

3.3. Technical Literature

Goodfellow et al. (2014) introduced generative adversarial networks, the architecture underlying early deepfake synthesis; **Westerlund (2019)** reviewed the technology's dual-use emergence; and **Mirsky and Lee (2021)** surveyed creation and detection techniques, documenting the arms-race dynamic in which detection persistently lags generation—a finding with direct consequences for forensic practice and the law of evidence.

3.4. Regulatory and Comparative Scholarship

A distinct strand evaluates regulatory design. **Kirchengast (2020)** analysed early criminalisation-and-control models and warned that platform self-regulation alone is structurally inadequate. **Meskys, Liaudanskas, Kalpokienė, and Jurcys (2020)** proposed a typology distinguishing malicious uses (notably non-consensual pornography) from legitimate synthetic-media uses, and argued for use-specific rather than technology-wide prohibition. **van der Sloot and Wagensveld (2022)** catalogued the regulatory dilemmas—definition, detection, jurisdiction, enforcement—that any deepfake regime must resolve. **Mania (2024)** compared European Union member-state protections for revenge-porn and deepfake-porn victims and found fragmentation and weak victim remedies even within a harmonising legal order, and **Romero Moreno (2024)** evaluated emerging AI-governance instruments, including transparency and provenance duties, against human-rights standards, cautioning that labelling obligations without victim remedies risk becoming compliance theatre.

3.5. Critical Synthesis

Read together, the literature converges on three propositions: that deepfake abuse is empirically gendered; that its core wrong is the violation of consent and sexual privacy rather than obscenity; and that platform-only regulation is insufficient without perpetrator liability and victim remedies. It diverges, however, on at least three questions. First, the criminalisation-of-creation debate: **Öhman (2020) and Viola and Voto (2023)** support liability for creation per se, while **Meskys et al. (2020)** and, implicitly, the American publication-centred model reflected in later federal law confine liability to distribution, fearing over-criminalisation of private conduct and thought-crime objections. Second, the speech-protection debate: **Chesney and Citron (2019)** and **Romero Moreno (2024)** emphasise the expressive and innovation costs of broad prohibitions, whereas the feminist literature emphasises the silencing effect of the abuse itself on women's expression—a conflict of speech interests, not a conflict between speech and its absence. Third, the remedial-design debate between criminal-law-centred and regulator-centred models, on which **Mania (2024)** and **Kirchengast (2020)** reach opposite emphases. The literature also has identifiable limitations for present purposes: it is dominated by United States, United Kingdom, European, and Australian material; its empirical base rarely includes South Asian populations; and almost none of it engages the post-2023 Indian statutory landscape. These limitations define the research gap that follows.

4. Research Gap

Stated precisely, prior scholarship has not done four things. First, no doctrinal study has evaluated deepfake abuse against the *replaced* Indian criminal architecture—the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Adhiniyam, all effective 1 July 2024—because the pre-2024 literature analysed the Indian Penal Code, the Code of Criminal Procedure, and the Indian Evidence Act, whose provisions, section numbers, and evidentiary certificates no longer govern. Second, no peer-reviewed study has analysed the Information Technology Amendment Rules, 2026 (G.S.R. 120(E)), which post-date the existing literature entirely; scholarship on Indian intermediary liability stops at the 2021–2023 rule amendments and the 2023 advisories. Third, the comparative literature (e.g., **Mania, 2024; Kirchengast, 2020**) benchmarks European, North American, and Australian regimes against each other but does not position India within that matrix,

despite India now operating one of the few binding synthetic-content labelling regimes in force anywhere. Fourth, the Indian doctrinal commentary that does exist is predominantly practitioner-oriented and descriptive; it has not applied an explicit theoretical framework—feminist legal theory and informational privacy—to generate evaluative criteria and a prioritised reform agenda for women victims specifically. This article addresses each of these four deficits.

5. Research Questions

The study is guided by five research questions:

- **RQ1.** What are AI-generated deepfakes, and how are they created and disseminated?
- **RQ2.** Why are women disproportionately targeted by deepfake abuse?
- **RQ3.** Does the existing Indian legal framework adequately regulate deepfake crimes against women?
- **RQ4.** What doctrinal, procedural, and institutional gaps persist in that framework?
- **RQ5.** What legal reforms are necessary, in light of international best practices, to secure effective protection and remedies for women victims?

6. Objectives

Corresponding to the research questions, the article pursues five objectives: to evaluate the existing statutory and constitutional framework applicable to deepfake abuse; to identify legislative, procedural, and enforcement gaps; to study judicial developments in the Supreme Court and High Courts bearing on synthetic media, privacy, personality rights, and non-consensual intimate imagery; to study international and comparative best practices; and to propose concrete, prioritised, and constitutionally sustainable legal reforms.

7. Methodology

7.1. Research Design

The study adopts doctrinal (black-letter) legal research based exclusively on secondary data, supplemented by comparative legal analysis. No surveys, interviews, questionnaires, or primary empirical data were used, and no statistic is reported that does not appear in an official publication or peer-reviewed source. The doctrinal method is applied in its conventional two-stage form: location and authentication of authoritative legal materials, followed by analysis through statutory interpretation, case synthesis, and normative evaluation against the criteria derived from the theoretical framework in Section 2.

7.2. Sources, Search Strategy, and Selection Criteria

Primary legal materials comprise the Constitution of India; central statutes as published on India Code; statutory rules and amendment notifications verified against the Gazette of India (eGazette); and judgments of the Supreme Court of India and the High Courts accessed through SCC OnLine and Manupatra and, where available, official court websites. Official governmental materials (MeitY notifications, advisories, and FAQs; NCRB "Crime in India" reports; Press Information Bureau releases) supply the regulatory and statistical context. International instruments (CEDAW and its General Recommendations; the Council of Europe's Convention on Cybercrime, 2001, discussed comparatively only, since India is not a party) and foreign legislation verified on official portals (legislation.gov.uk, legislation.gov.au, congress.gov, EUR-Lex) provide the comparative frame. Peer-reviewed literature was identified through Scopus, HeinOnline, JSTOR, SSRN, and Google Scholar using the keywords "deepfake", "synthetically generated information", "non-consensual intimate imagery", "image-based sexual abuse", "morphed images", "personality rights", and "intermediary liability". Inclusion criteria: enacted statutes and notified rules; reported judgments; official reports; ratified international instruments; and peer-reviewed journal literature. Exclusion criteria: draft bills and proposals (except where expressly flagged as ongoing policy debate); blogs and opinion pieces; unverifiable statistics; and media reportage, which was used for orientation only and never as authority. Every authority cited was cross-checked against its official source, and matters that remain unsettled—pending implementation, proposed amendments, or anticipated litigation—are identified as such in the text. Figure 5 depicts the design.

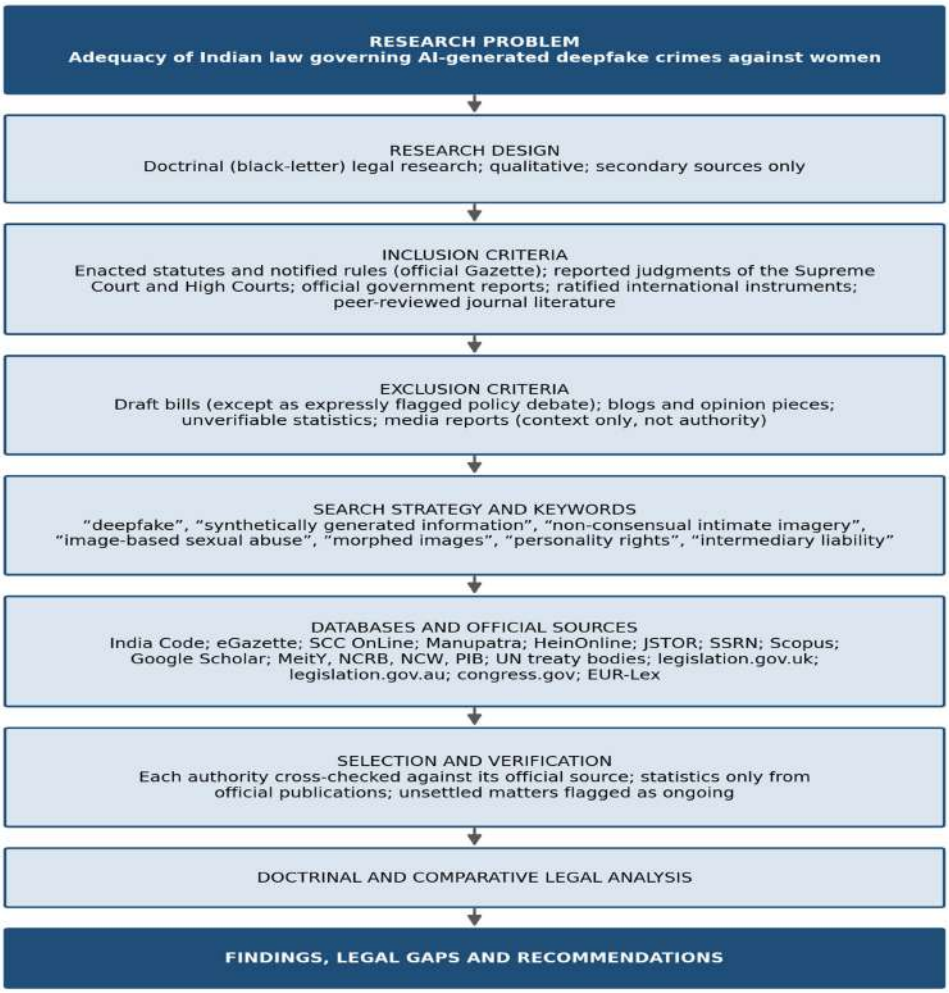

Figure-5: Research methodology: doctrinal design, sources, inclusion and exclusion criteria, and analysis.

8. Understanding AI Deepfake Technology

8.1. Artificial Intelligence and Deep Learning

Artificial intelligence, in the sense relevant here, denotes computational systems that perform tasks ordinarily associated with human cognition—perception, pattern recognition, and content generation—by learning statistical regularities from data. Deep learning, a subset of machine learning, employs multi-layered artificial neural networks trained on large datasets. Generative models within this paradigm do not merely classify inputs; they synthesise new outputs that resemble their training data. The pivotal architecture was the generative adversarial network (GAN), in which a "generator" network fabricates samples and a "discriminator" network attempts to distinguish fabrications from genuine data, each improving through adversarial training until the generator's outputs become highly realistic (Goodfellow et al., 2014). Subsequent techniques—autoencoder-based face-swapping, voice-cloning models, and, more recently, diffusion models—have progressively lowered the technical skill, data, and computing resources required to produce convincing synthetic media (Mirsky & Lee, 2021).

8.2. Meaning and Creation of Deepfakes

The term "deepfake"—a portmanteau of "deep learning" and "fake"—originated in late 2017 from an online forum account that used face-swapping software to insert female celebrities' faces into pornographic videos (Chesney & Citron, 2019). Technically, deepfake creation typically involves: (i) collection of images, video, or voice samples of the target, frequently scraped from social media without consent; (ii) training or fine-tuning of a generative model on that data; (iii) synthesis, in

which the target's likeness is mapped onto source material or generated outright; and (iv) post-processing to remove artefacts **(Mirsky & Lee, 2021; Westerlund, 2019)**. Contemporary consumer applications compress this pipeline into a few clicks, and so-called "nudify" services generate sexualised imagery from a single ordinary photograph. Indian law now captures this class of output through the regulatory definition of "synthetically generated information" inserted as Rule 2(1)(wa) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, by the 2026 Amendment Rules: audio, visual, or audio-visual information that is artificially or algorithmically created, generated, modified, or altered using a computer resource in a manner that appears reasonably authentic or true **(MeitY, 2026a)**. Figure 1 depicts the lifecycle from creation to legal remedy.

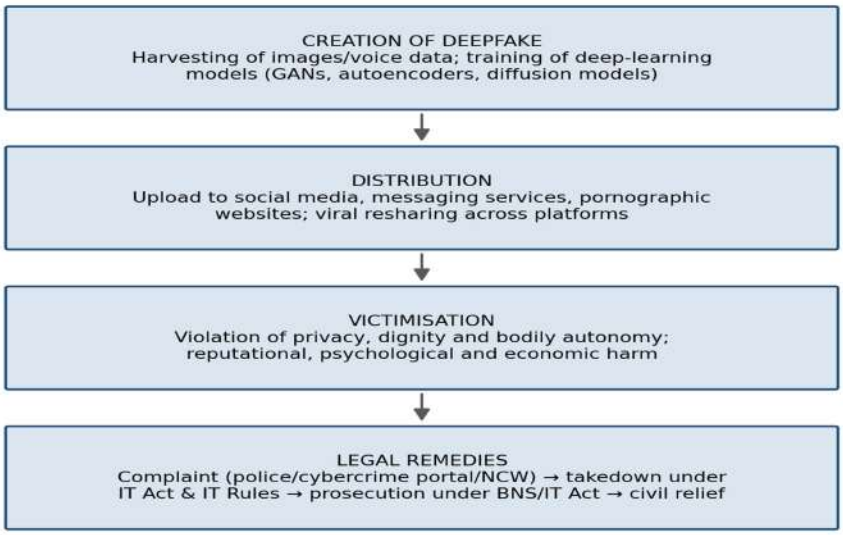

Figure-1: Lifecycle of deepfake abuse: creation, distribution, victimisation, and legal remedies.

9. Deepfake Crimes Against Women

9.1. Women as Primary Victims

The gendered distribution of deepfake harm is empirically established. Auditing 14,678 deepfake videos online in 2019, Ajder et al. found that 96% were pornographic and that the subjects on the top deepfake pornography websites were exclusively women **(Ajder et al., 2019)**; subsequent multi-country research confirms both prevalence and gendered targeting **(Flynn et al., 2022; Umbach et al., 2024)**. This distribution is not accidental. Image-based sexual abuse operates as a technology of gendered control: it sexualises women without consent, weaponises cultural norms of female modesty and "honour", and imposes silencing costs on women's participation in public life **(Citron & Franks, 2014; McGlynn & Rackley, 2017)**, a silencing function that extends from pornographic to overtly political deepfakes targeting women **(Maddocks, 2020)**. In the Indian social context, where family reputation and community perception weigh heavily on women, even a demonstrably fabricated intimate image can trigger social ostracism and matrimonial, educational, and employment consequences. CEDAW General Recommendation No. 35 (2017) recognises that gender-based violence against women occurs in all spaces of human interaction, including technology-mediated environments, and reiterates states' due-diligence obligations to prevent, investigate, punish, and provide reparation for such violence **(CEDAW Committee, 2017)**.

9.2. The Indian Statistical Context

Official Indian crime statistics do not yet record "deepfake" as a distinct head, so the phenomenon must be situated within the NCRB's cybercrime series, read with its motive-wise breakdown, and with two well-documented caveats: registered crime substantially understates incidence, particularly for sexual and image-based offences where stigma suppresses reporting **(Henry & Powell, 2018)**,

and year-on-year changes partly reflect reporting infrastructure such as the National Cybercrime Reporting Portal rather than underlying incidence alone. Within those limits, the trend is unambiguous: registered cybercrime grew every year from 2019 to 2023, rising 31.2% in 2023 alone to 86,420 cases, with the cybercrime rate per lakh population increasing from 4.8 to 6.2; within the 2023 total, sexual exploitation was the recorded motive in 4,199 cases (4.9%), and cases of cheating by personation under the IT Act nearly doubled over the previous year **(NCRB, 2023, 2025)**. Table 1 presents the series. The 2024 report had not been published at the time of writing; the trend for that year is accordingly not asserted.

Table-1: Registered Cybercrime in India, 2019–2023 (NCRB "Crime in India" Series)

Year	Cybercrime cases registered	Change over previous year	Rate per lakh population	Recorded motive: sexual exploitation
2019	44,735	+63.5%	3.3	2,266 (5.1%)
2020	50,035	+11.8%	3.7	3,293 (6.6%)
2021	52,974	+5.9%	3.9	4,555 (8.6%)
2022	65,893	+24.4%	4.8	3,648 (5.5%)
2023	86,420	+31.2%	6.2	4,199 (4.9%)

Source. Compiled by the author from National Crime Records Bureau, Crime in India reports for the respective years **(NCRB, 2020, 2021, 2022, 2023, 2025)**, Ministry of Home Affairs, Government of India. Figures are cases registered under cybercrimes (IT Act, and IPC/BNS and SLL offences involving communication devices as medium/target); motive-wise figures as reported by NCRB.

9.3. Typology of Deepfake Offending

Deepfake abuse against women manifests in overlapping forms: deepfake pornography and other non-consensual intimate imagery (NCII); sextortion, in which fabricated imagery is used to coerce victims into payment, sexual acts, or silence; cyber harassment and cyberstalking amplified by synthetic content; identity theft and impersonation through cloned profiles, voices, and videos; defamation and reputational attacks, including politically motivated attacks on women journalists and public figures; and fraud facilitated by voice cloning. Each form implicates distinct statutory provisions, which partly explains the fragmentation of the Indian legal response examined below. The psychological literature documents harms—anxiety, depression, post-traumatic stress symptoms, and social withdrawal—comparable to those following physical sexual offences **(McGlynn, Rackley, & Houghton, 2017)**. Figure 2 maps the typology.

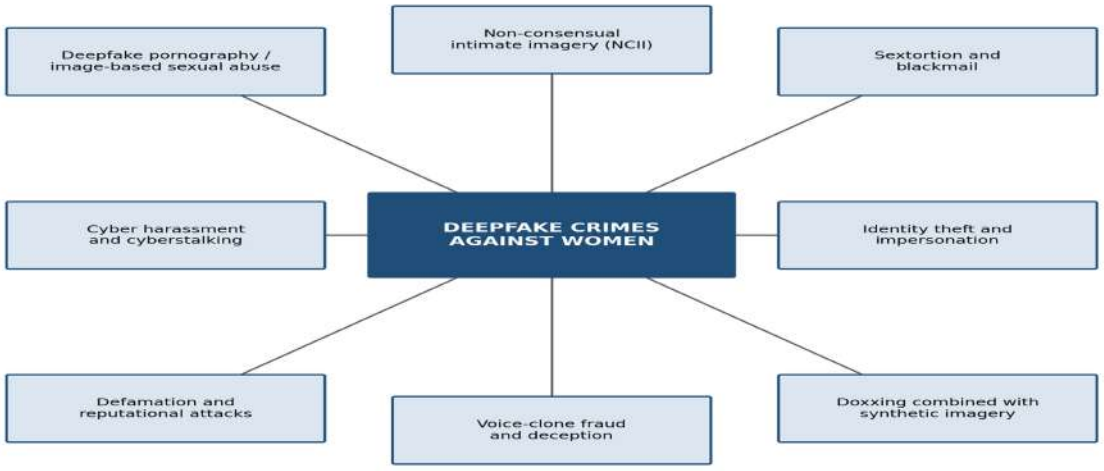

Figure-2: Typology of deepfake crimes against women.

9.4. Consent as the Organising Principle

A conceptual point with doctrinal consequences must be emphasised: the wrong in synthetic NCII is the absence of consent to sexualised representation, not the falsity or obscenity of the image. A defence that the depicted acts "never happened" does not answer the violation of the woman's sexual autonomy, dignity, and informational self-determination **(Citron, 2019; Viola & Voto, 2023)**. Provisions organised around obscenity (which protect public morality) or defamation (which protect reputation and admit truth-related defences) therefore capture the harm only obliquely. This misalignment, identified in the comparative literature **(Chesney & Citron, 2019; McGlynn & Rackley, 2017)**, recurs throughout the analysis of Indian law that follows.

10. The Indian Legal Framework

India regulates deepfake abuse through five instruments of general application, summarised in Table 2 and depicted hierarchically in Figure 3. Consistently with the distinction drawn in the Introduction, it must be stated at the outset—and this is itself a central finding—that no Act of Parliament mentions deepfakes or synthetic media; the concept enters Indian law only through subordinate legislation, namely the 2026 amendments to the intermediary rules.

10.1. Information Technology Act, 2000

The IT Act supplies the principal cyber-specific offences. Section 66C penalises fraudulent or dishonest use of another person's electronic signature, password, or "any other unique identification feature" (imprisonment up to three years and fine), and is invocable where a woman's likeness or identity credentials are appropriated. Section 66D punishes cheating by personation using a computer resource, apt for deepfake impersonation frauds. Section 66E criminalises the intentional capture, publication, or transmission of an image of the "private area" of a person without consent, under circumstances violating privacy; its language, drafted for voyeurism involving real images, generates interpretive difficulty where the depicted body is synthetic even though the face is real. Sections 67 and 67A punish publication or transmission of obscene and sexually explicit electronic material respectively, and Section 67B addresses child sexual abuse material. These are the provisions most commonly invoked against deepfake pornography, yet they are obscenity offences: they require the material to be lascivious or sexually explicit, and they do not make the victim's non-consent an ingredient.

Two structural provisions complete the Act's architecture. Section 69A empowers the Central Government to direct blocking of public access to information, a power whose constitutionality was upheld in *Shreya Singhal v. Union of India* (2015). Section 79 confers conditional immunity ("safe harbour") on intermediaries for third-party content, contingent on due diligence and expeditious removal upon actual knowledge; *Shreya Singhal* confined "actual knowledge" to receipt of a court order or notification from the appropriate government agency.

10.2. The Intermediary Rules and the 2026 SGI Amendments

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified vide G.S.R. 139(E) dated 25 February 2021 under Section 87(1) and clauses (z) and (zg) of Section 87(2) of the IT Act, operationalise Section 79 due diligence, and have been amended vide G.S.R. 794(E) dated 28 October 2022, G.S.R. 275(E) dated 6 April 2023, G.S.R. 775(E) dated 22 October 2025, and G.S.R. 120(E) dated 10 February 2026 **(MeitY, 2026a)**. Rule 3(1)(b) obliges intermediaries to make reasonable efforts to prevent users from hosting specified categories of unlawful content, and Rule 3(2)(b) has, since 2021, required removal within twenty-four hours of complaints concerning content exposing private areas, depicting nudity or sexual acts, or artificially morphed images impersonating a person—one of the few pre-2026 provisions expressly contemplating morphed imagery. Following the viral circulation of deepfake videos of film actresses, MeitY issued advisories on 7 November 2023 and 26 December 2023 reminding intermediaries that impersonation, including through artificially morphed images, attracts existing removal obligations, and in March 2024 issued a further advisory concerning the deployment of under-tested AI models **(MeitY, 2023; PIB, 2024)**.

The decisive development is the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified in the Gazette of India, Extraordinary, Part II, Section 3(i), vide G.S.R. 120(E) dated 10 February 2026 and in force from 20 February 2026, following draft proposals published for consultation in October 2025 **(MeitY, 2026a, 2026b)**. Substantively, the Amendment Rules do six things. First, they define "synthetically generated information" in Rule 2(1)(wa) in technology-neutral terms, with express carve-outs for routine and good-faith editing and document creation. Second, they require intermediaries whose computer resources could enable creation or dissemination of SGI to deploy reasonable and appropriate technical measures, including automated tools, to prevent specified unlawful content, expressly including non-consensual intimate imagery and obscene or sexually explicit material (new Rule 3(3)). Third, they mandate that permissible SGI be clearly and prominently labelled, with embedded permanent metadata or unique identifiers where feasible, and prohibit intermediaries from enabling removal or suppression of such labels or metadata.

Fourth, the newly inserted Rule 4(1A) requires significant social media intermediaries, before publication, to obtain user declarations as to whether uploaded content is SGI, to deploy appropriate technical measures to verify those declarations, and to label confirmed SGI—converting what was previously an "endeavour" standard into a compliance obligation, with a proviso that knowingly permitting, promoting, or failing to act on unlawful SGI is deemed a failure of due diligence. Fifth, the Rules compress timelines throughout: removal within three hours (previously thirty-six) of actual knowledge under Rule 3(1)(d), arising from a court order or a reasoned written intimation of an officer of the appropriate government not below the rank of Joint Secretary—or, where the intimation is issued by the police administration, of one or more officers each not below the rank of Deputy Inspector General of Police—subject to monthly review of such intimations at Secretary level; removal within two hours (previously twenty-four) of complaints under Rule 3(2)(b) concerning private-area exposure, nudity, sexual acts, or impersonation including artificially morphed images; and resolution of general grievances within seven days (previously fifteen), with removal-type complaints acted on within thirty-six hours (previously seventy-two). Sixth, Rule 2(1B) clarifies that good-faith removal in compliance with the Rules, including through automated measures, does not forfeit safe harbour under Section 79 **(MeitY, 2026a, 2026b)**.

Two further insertions are directly victim-facing. Rule 3(1)(ca) obliges intermediaries whose tools enable SGI creation to warn users that generating unlawful synthetic content may attract punishment under, inter alia, the BNS, the Protection of Children from Sexual Offences Act, 2012, the Indecent Representation of Women (Prohibition) Act, 1986, the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, and the Immoral Traffic (Prevention) Act, 1956—the first express linkage in the intermediary rules between synthetic media and the women-protection statutes—and that violations may lead to removal, account suspension without vitiating evidence, and, in accordance with applicable law, disclosure of the violating user's identity to a complainant who is the victim or acting on the victim's behalf. Rule 3(1)(cb) requires expeditious action once an intermediary becomes aware of such violations on its own accord, without awaiting formal notice. All provisions described in this subsection have been verified against the official consolidated text of the Rules as updated on 10 February 2026, published by **MeitY (2026a)**.

Two proposals remained unfinalised at the time of writing and are noted strictly as ongoing policy debate rather than law. The first concerns continuous on-screen display of SGI labels. The second is more consequential for the argument developed in Section 15: draft Second Amendment Rules circulated in March 2026 would leave the SGI provisions untouched but insert a new Rule 3(4) obliging intermediaries to comply with any clarification, advisory, order, direction, standard operating procedure, code of practice, or guideline issued by the Ministry regarding implementation of Part II, and would make such compliance part of the due-diligence obligations conditioning safe harbour under

Section 79 (MeitY, 2026c). That draft bears neither a Gazette number nor a commencement date and may be modified or abandoned; if notified in its present form, however, it would convert executive guidance into a safe-harbour condition, deepening rather than resolving the constitutional concerns identified below.

For women victims, the two-hour removal window for synthetic intimate imagery is arguably the most consequential platform-facing change so far, because the primary harm of NCII is a function of the speed and breadth of dissemination; measured against the forty-eight-hour window of the United States federal scheme and the non-numerical "expeditious" standards of the European regime discussed in Section 13, it is also among the shortest mandated removal timelines currently in force in any major jurisdiction. Nevertheless, the amendments regulate platforms, not perpetrators: the identity-disclosure mechanism of Rule 3(1)(ca) may assist a victim in locating her abuser, but the Rules themselves create no offence, no compensation, and no cause of action against the creator of the content. Their vires also remain contestable—subordinate legislation cannot exceed the rule-making power conferred by the parent Act, and industry bodies and commentators have questioned whether obligations of this breadth require parliamentary legislation. That debate, and any judicial review of the Rules, remained unresolved at the time of writing.

10.3. Digital Personal Data Protection Act, 2023

The DPDP Act, 2023, establishes a consent-centred regime for processing digital personal data. A woman's facial images and voice are personal data; scraping them to train a model and generate a deepfake without consent is processing without a lawful basis, exposing a data fiduciary to substantial monetary penalties imposed by the Data Protection Board. Three limitations, however, curtail the Act's utility for deepfake victims. First, the Act imposes penalties payable to the state but confers no statutory right to compensation on the affected individual—a regression from the now-omitted Section 43A of the IT Act, which had permitted compensation for negligent handling of sensitive personal data. Second, Section 3(c)(ii) excludes from the Act's scope personal data made publicly available by the data principal herself, an exclusion whose application to images scraped from public social-media profiles for deepfake creation is untested and troubling. Third, the Act's enforcement architecture is only now being operationalised: the Digital Personal Data Protection Rules, 2025, were notified in November 2025 with phased implementation, so the regime's practical efficacy remains to be demonstrated. These observations concern the framework as it stands at the time of writing; its trajectory is a matter of ongoing implementation rather than settled practice.

10.4. Bharatiya Nyaya Sanhita, 2023

The BNS, in force from 1 July 2024, supplies the general criminal law. Provisions applicable to deepfake abuse against women include: Section 75 (sexual harassment); Section 77 (voyeurism—watching or capturing the image of a woman engaging in a private act); Section 78 (stalking, including monitoring a woman's use of the internet or electronic communication); Section 79 (word, gesture, or act intended to insult the modesty of a woman); Section 294 (sale, distribution, or public exhibition of obscene material, expressly including material in electronic form); Section 318 (cheating); Section 319 (cheating by personation); Section 336 (forgery, including of electronic records, with aggravated forms where the forgery is intended to harm reputation); Section 351 (criminal intimidation, apt for sextortion threats); and Section 356 (defamation).

This battery is real but ill-fitting. Voyeurism under Section 77 presupposes observation or capture of a woman actually engaged in a private act, which a wholly fabricated depiction is not. Forgery requires the making of a false document or electronic record with intent to cause damage or injury, and prosecutions must persuade courts that a synthetic video is a "false electronic record" in the statutory sense. Defamation is centred on reputation and admits truth-related defences, mischaracterising the sexual-autonomy violation. No BNS provision names the creation or distribution of non-consensual intimate imagery—authentic or synthetic—as a distinct offence.

10.5. Procedure and Evidence: BNSS and BSA, 2023

The BNSS modernises procedure with relevance for cyber investigation: it permits summons and production of electronic communication and devices (Section 94), mandates audio-video recording of search and seizure (Section 105), and requires forensic expert visits to crime scenes for offences punishable with seven years or more (Section 176(3)). The BSA restructures the law of electronic evidence: Sections 61 to 63 govern admissibility of electronic records, with Section 63 **(successor to Section 65B of the Indian Evidence Act, 1872)** requiring a certificate for electronic evidence, now accompanied by an expert-supported certificate format. These reforms assist deepfake prosecutions in principle, but as discussed in Section 14, forensic authentication of synthetic media—proving that a video is fabricated, and attributing its creation—remains the operational bottleneck.

Table-2: Existing Indian Laws Applicable to AI-Generated Deepfake Crimes Against Women

Instrument	Key Provisions	Application to Deepfake Abuse	Principal Limitation
Constitution of India	Arts. 14, 15, 19, 21	Privacy, dignity, informational self-determination **(Puttaswamy, 2017)**; reputation as an Art. 21 facet **(Subramanian Swamy, 2016)**	Rights primarily vertical; horizontal reach evolving **(Kaushal Kishor, 2023)**
IT Act, 2000	Ss. 66C, 66D, 66E, 67, 67A, 69A, 79	Identity theft; impersonation fraud; privacy-violating images; obscene/sexually explicit content; blocking; intermediary safe harbour	Obscenity-centred; consent not an ingredient; no mention of synthetic media
IT Rules, 2021 (as amended up to G.S.R. 120(E), 2026)	R. 2(1)(wa), 3(1)(b), 3(2)(b), 3(3), 4(1A)	SGI definition; labelling and metadata; 2-hr removal of synthetic NCII; 3-hr takedown on lawful orders; SSMI verification duties	Subordinate legislation; regulates platforms only; no offence, no victim compensation; vires debated
DPDP Act, 2023	Consent-based processing; penalties on fiduciaries; DPDP Rules, 2025	Non-consensual scraping and processing of images/voice as personal-data violation	No individual compensation; publicly-available-data exclusion (s. 3(c)(ii)); phased enforcement
BNS, 2023	Ss. 75, 77, 78, 79, 294, 318, 319, 336, 351, 356	Harassment, voyeurism, stalking, obscenity, personation, forgery, intimidation, defamation	No dedicated NCII/deepfake offence; provisions drafted for authentic content
BNSS & BSA, 2023	BNSS ss. 94, 105, 176(3); BSA ss. 61–63	Digital investigation powers; admissibility and certification of electronic records	Forensic capacity and authentication of synthetic media remain constrained

Source. Compiled by the author from the bare Acts as published on India Code, the Gazette notifications of the IT Rules and their amendments (G.S.R. 139(E)/2021; G.S.R. 794(E)/2022; G.S.R. 275(E)/2023; G.S.R. 775(E)/2025; G.S.R. 120(E)/2026), and the judgments cited.

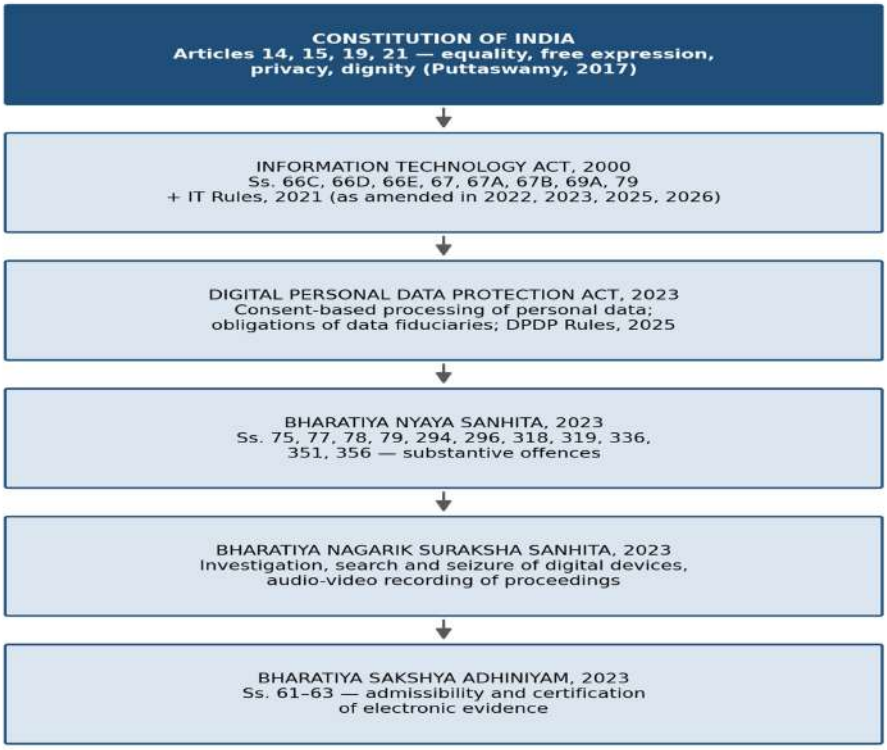

Figure-3: Hierarchy of the Indian legal framework governing deepfake abuse.

11. Constitutional Perspective

The constitutional foundation of the deepfake victim's claim is the right to privacy recognised as intrinsic to Article 21 by a nine-judge Bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1. *Puttaswamy* articulated privacy as encompassing bodily autonomy, informational privacy, and decisional autonomy, and recognised the individual's interest in controlling the dissemination of personal information. A deepfake constructed from a woman's harvested images violates each facet: it appropriates her informational identity, fabricates her bodily presentation, and negates her decisional control over sexual self-representation. The five-judge decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2019) 1 SCC 1, upholding the Aadhaar framework in part, added the operative discipline: interferences with informational privacy must satisfy the tests of legality, legitimate aim, and proportionality—a template equally applicable to state regulation of synthetic media and to the design of intermediary obligations.

Three further Supreme Court decisions complete the constitutional matrix. In *Subramanian Swamy v. Union of India* (2016) 7 SCC 221, the Court upheld criminal defamation and, significantly for present purposes, located the right to reputation within Article 21, holding that one person's freedom of expression cannot extinguish another's dignity and reputation; a sexualised deepfake is simultaneously an attack on reputation in this constitutional sense and something more—an appropriation of the person herself. In *Navtej Singh Johar v. Union of India* (2018) 10 SCC 1, the Court grounded decriminalisation in the constitutional values of dignity, autonomy, and identity, articulating sexual autonomy as constitutionally protected self-determination; that articulation supplies the precise vocabulary for the wrong in synthetic NCII, which negates the victim's authorship of her own sexual representation.

In *Kaushal Kishor v. State of Uttar Pradesh* (2023) 4 SCC 1, a Constitution Bench held that the fundamental rights under Articles 19 and 21 are enforceable even against persons other than the State—a development of direct relevance to a harm inflicted almost entirely by private actors through private platforms, and one that strengthens the constitutional case for horizontal statutory protection. Articles 14 and 15 are engaged by the demonstrably

disproportionate targeting of women, permitting—indeed inviting—gender-responsive legislative classification, and Article 51A(e), which casts a fundamental duty to renounce practices derogatory to the dignity of women, supplies interpretive support.

Countervailing constitutional constraints are equally important. Article 19(1)(a) protects expression, including satire, parody, and artistic uses of synthetic media, and restrictions must fall within the grounds of Article 19(2) and satisfy the proportionality analysis of the *Puttaswamy* decisions. *Shreya Singhal* (2015) 5 SCC 1 is the cautionary precedent: Section 66A of the IT Act was invalidated for vagueness and overbreadth, and any future deepfake offence drafted in loose terms ("misleading", "offensive", "harmful") would court the same fate. The constitutional path is therefore a narrowly drawn offence centred on non-consensual intimate or sexual depiction of an identifiable person, rather than a general prohibition of synthetic media. The compressed takedown timelines of the 2026 Rules will likely face proportionality scrutiny on this axis: a two-hour window for synthetic NCII is defensible given the irreversibility of dissemination; a three-hour window for all unlawful content, enforced through safe-harbour forfeiture, raises the spectre of over-removal and private censorship that *Shreya Singhal* sought to contain. This tension is identified here as an open constitutional question, not settled law.

12. Judicial Analysis

12.1. Non-Consensual Intimate Imagery: The Mrs X Framework

The most consequential Indian judicial engagement with NCII to date is *Mrs X v. Union of India*, 2023 SCC OnLine Del 2361 (Delhi High Court, 26 April 2023). The petitioner's intimate images, captured under coercion, were repeatedly re-uploaded to pornographic websites despite complaints to platforms and the cybercrime portal. Justice Subramonium Prasad, anchoring the analysis in *Puttaswamy* and the right to informational privacy, and drawing on the Kerala High Court's right-to-be-forgotten jurisprudence in *Vysakh K.G. v. Union of India*, issued systemic directions: search engines must de-index offending content on a token or digital-identifier basis so that victims are not forced to return to court for every re-upload; they must deploy existing hash-matching technology to prevent resurfacing; intermediaries must prominently display the Rule 3(2)(b) reporting mechanism; strict adherence to the rule's timelines is a condition of Section 79 safe harbour; the cybercrime portal must provide a status tracker; and police must promptly register and investigate complaints. Although the case concerned authentic imagery, its architecture—victim-initiated, re-upload-proof, timeline-enforced removal—prefigured the 2026 amendments and applies with equal force to synthetic NCII, which falls squarely within Rule 3(2)(b)'s reference to artificially morphed images. *Mrs X* is thus the doctrinal bridge between the constitutional right and the regulatory machinery.

12.2. Personality Rights and Synthetic Media

A parallel line of civil authority protects identity against synthetic appropriation. In *Anil Kapoor v. Simply Life India*, CS(COMM) 652/2023 (Delhi High Court, 2023), the Court granted an omnibus interim injunction protecting the actor's name, likeness, image, and voice against unauthorised exploitation, expressly encompassing misuse through artificial-intelligence tools and deepfakes, while preserving satire and parody as protected expression. The decision extended the personality-rights line of *Amitabh Bachchan v. Rajat Nagi*, CS(COMM) 819/2022 (Delhi High Court, 2022). In *Jaikishan Kakubhai Saraf (Jackie Shroff) v. The Peppy Store*, CS(COMM) 389/2024 (Delhi High Court, 2024), protection was extended against misuse across e-commerce listings and AI chatbots. The Bombay High Court joined this development in *Arijit Singh v. Codible Ventures LLP* (order dated 26 July 2024), restraining AI voice-cloning tools that converted text and audio into the singer's cloned voice, and expressly warning that generative-AI tools enable misappropriation of a performer's identity; further interim orders protecting public figures against deepfake and morphed content followed in 2025, including in favour of Aishwarya Rai Bachchan and Abhishek Bachchan.

Two observations temper this line's significance for the present inquiry. These are civil, celebrity-driven remedies—injunctions

grounded in publicity, passing off, and dignity—realistically available only to litigants of means; and they protect identity as quasi-property more readily than they vindicate sexual autonomy. Their doctrinal value nonetheless lies in consistent judicial recognition that AI-fabricated likenesses are actionable violations of Article 21 interests.

12.3. Public Law, Trial-Level Practice, and the Supreme Court's Silence

In the public-law docket, *Chaitanya Rohilla v. Union of India*, W.P.(C) 15596/2023, and *Rajat Sharma v. Union of India*, W.P.(C) 6560/2024 (Delhi High Court), sought directions to regulate deepfakes and block deepfake-generation services; in November 2024 the Court recorded the constitution of a MeitY committee to examine the problem and recommend measures, and the October 2025 draft amendments and the February 2026 Amendment Rules followed this process. The Court's posture—prodding executive rule-making rather than judicially legislating—illustrates both the utility and the limits of public interest litigation in technology governance. At trial level, convictions for online circulation of a victim's intimate images have been secured under the IT Act's provisions read with penal-code offences, of which the prosecution in *State of West Bengal v. Animesh Boxi* (Court of Sessions, West Bengal, 2018) is the most frequently cited early example, albeit a Sessions Court decision without precedential force. No Supreme Court judgment has yet ruled directly on deepfakes or synthetic NCII; the constitutional principles of Section 11 therefore await authoritative application to this technology, and the overall judicial picture is of doctrinally creative but structurally stop-gap adjudication pending legislative consolidation.

13. Comparative Study

13.1. International Framework

At the international level, no treaty addresses deepfakes by name, but binding and persuasive instruments frame state obligations. The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW, 1979), which India ratified in 1993, obliges states parties to eliminate discrimination against women; the CEDAW Committee's General Recommendation No. 19 (1992) established gender-based violence as a form of discrimination, and General Recommendation No. 35 (2017) updated that framework, expressly recognising that such violence manifests in technology-mediated settings and reiterating the due-diligence standard for acts of private actors. Article 17 of the International Covenant on Civil and Political Rights, ratified by India in 1979, protects against arbitrary or unlawful interference with privacy, honour, and reputation. The Council of Europe's Convention on Cybercrime (Budapest Convention, 2001) is the principal instrument on procedural cooperation in cybercrime—expedited preservation of stored data, mutual legal assistance, and transborder access; India is not a party, a position it has maintained citing sovereignty concerns and its non-participation in the drafting, and this abstention complicates cross-border evidence gathering in deepfake cases whose infrastructure is typically foreign-hosted. The discussion of the Convention here is accordingly comparative and analytical only. Table 3 summarises the international framework.

Table-3: International Legal Framework Relevant to Deepfake Abuse of Women

Instrument	Status for India	Relevance
CEDAW, 1979	Ratified 1993 (with declarations)	Non-discrimination; due-diligence obligation for gender-based violence, including technology-facilitated violence (GR 19, 1992; GR 35, 2017)
CEDAW General Recommendations 19 & 35	Authoritative Committee interpretation	Frame online image-based abuse as gender-based violence requiring prevention, protection, prosecution, and reparation
ICCPR, 1966 (Art. 17)	Ratified 1979	Protection against arbitrary or unlawful interference with privacy, honour, and reputation
Budapest Convention, 2001	Not a party	Model for procedural powers and international cooperation in electronic-evidence gathering (comparative reference only)
UN Women / UNESCO studies	Persuasive institutional material	Document prevalence and chilling effect of online violence against women, including manipulated imagery

Source. Compiled by the author from United Nations treaty texts and Committee documents (CEDAW/C/GC/35), the Council of Europe treaty office (ETS No. 185), and India's ratification record.

13.2. European Union

The EU regulates synthetic media through a lattice of instruments rather than a single deepfake statute. The Artificial Intelligence Act (Regulation (EU) 2024/1689) adopts a transparency approach: Article 50 obliges deployers of AI systems that generate or manipulate image, audio, or video content constituting a deepfake to disclose that the content has been artificially generated or manipulated, with machine-readable marking obligations on providers of generative systems. The General Data Protection Regulation supplies rights against non-consensual processing of biometric and image data, including erasure. The Digital Services Act (Regulation (EU) 2022/2065) imposes notice-and-action obligations on hosting services and systemic-risk assessment and mitigation duties on very large online platforms, which encompass the dissemination of illegal content such as image-based sexual abuse. Decisively, Directive (EU) 2024/1385 on combating violence against women and domestic violence requires member states to criminalise, inter alia, the non-consensual production or manipulation—including by means of artificial intelligence—and subsequent public dissemination of material making it appear that a person is engaged in sexual activities, with transposition timelines extending to 2027. The EU model therefore combines AI transparency, data protection, platform accountability, and a harmonised criminal offence, although **Mania's (2024)** comparative findings caution that member-state implementation of victim protection remains uneven.

13.3. United Kingdom

The United Kingdom moved in two steps. The Online Safety Act 2023 (c. 50) replaced the older disclosure offences with a modernised set of intimate-image offences inserted into the Sexual Offences Act 2003 **(sections 66A to 66D)**, criminalising the sharing of, and threats to share, intimate images without consent, in terms expressly extending to images that appear to be of the person, including altered and AI-generated material—thereby covering sexual deepfakes—while also imposing statutory duties of care on platforms enforced by Ofcom. The Data (Use and Access) Act 2025 (c. 18) then closed the remaining gap: section 138 inserts sections 66E to 66H into the Sexual Offences Act 2003, creating offences of creating, and of requesting the creation of, a "purported intimate image" of an adult without consent or reasonable belief in consent; the offences were

brought into force on 6 February 2026 by the Data (Use and Access) Act 2025 (Commencement No. 5) Regulations 2026 (S.I. 2026/31). The UK thus criminalises creation, solicitation, and distribution on a consent basis, decoupled from the motive requirements that had hampered earlier prosecutions.

13.4. United States

After years of state-level patchwork, the United States enacted the TAKE IT DOWN Act (S. 146, 119th Congress; Public Law No. 119-12), signed into law on 19 May 2025. The Act criminalises knowingly publishing, via an interactive computer service, non-consensual intimate visual depictions of identifiable adults, and "digital forgeries"—computer-generated intimate depictions—of identifiable individuals, with penalties of up to two years' imprisonment for offences involving adults and three years involving minors, and separate liability for threats to publish. Its second pillar mandates that covered platforms operate a notice-and-removal process: upon a valid request from the depicted individual, the platform must remove the depiction within forty-eight hours and make reasonable efforts to remove identical copies, with non-compliance enforced by the Federal Trade Commission as an unfair or deceptive practice; the platform obligations took effect on 19 May 2026 **(Congressional Research Service, 2025)**. The Act does not preempt state statutes—now enacted in the great majority of states—addressing NCII and sexual deepfakes, and its publication-centred design leaves the criminalisation of creation largely to state law.

13.5. Australia

Australia's Criminal Code Amendment (Deepfake Sexual Material) Act 2024 (Cth) amended the federal Criminal Code to criminalise the transmission of sexual material depicting an adult, using a carriage service, without consent, in terms expressly covering material created or altered using technology, including deepfakes, with imprisonment of up to six years and an aggravated offence of up to seven years where the person also created or altered the material. This criminal regime operates alongside the civil scheme of the Online Safety Act 2021 (Cth), under which the eSafety Commissioner administers a complaints-based image-based-abuse removal mechanism with rapid takedown powers and civil penalties—an institutional model of a dedicated online-safety regulator that India lacks.

13.6. Comparative Assessment

Three convergent design features emerge across these jurisdictions, as summarised in Table 4 and Figure 4: (i) a dedicated, narrowly drawn criminal offence of non-consensual synthetic intimate imagery, increasingly covering creation as well as distribution; (ii) a statutory, victim-initiated platform takedown mechanism with short, enforceable deadlines and an identified regulator; and (iii) transparency obligations (labelling, provenance metadata) imposed on generative-AI providers and platforms. India, after the 2026 Amendment Rules, possesses a strong version of the third feature and a partial, subordinate-legislation version of the second, but entirely lacks the first. The divergences in the comparative record are equally instructive for Indian drafting choices: the UK and, in aggravated form, Australia criminalise creation, while the US federal scheme is publication-centred—the very disagreement identified in the literature **(Meskys et al., 2020; Viola & Voto, 2023)**—and enforcement architecture ranges from a dedicated regulator (Australia, UK) to a general consumer-protection agency (US).

ISSN: 2583-7354

Table-4: Comparative Legal Regulation of AI-Generated Deepfake Abuse: India, EU, UK, USA, Australia

Parameter	India	European Union	United Kingdom	United States	Australia
Dedicated deepfake-NCII offence	No	Yes (Directive (EU) 2024/1385; transposition to 2027)	Yes **(sharing: OSA 2023, c. 50; creation: DUAA 2025, c. 18, s. 138)**	Yes **(TAKE IT DOWN Act, Pub. L. 119-12)**	Yes **(Deepfake Sexual Material Act 2024 (Cth))**
Creation criminalised	No	Production/manipulation covered by Directive	Yes **(SOA 2003, ss. 66E–66F, in force 6 Feb 2026)**	Publication-centred; creation via state laws	Aggravated offence where creator
Platform takedown duty	IT Rules: 2 hrs (synthetic NCII), 3 hrs (lawful orders)	DSA notice-and-action; VLOP risk duties	OSA duties of care (Ofcom)	48-hr notice-and-removal (FTC)	eSafety removal scheme
AI transparency/labelling	Yes **(SGI labelling, G.S.R. 120(E), 2026)**	Yes **(AI Act, Art. 50)**	No general labelling statute	No general federal labelling statute	No general labelling statute
Victim civil remedy/compensation	General tort/constitutional remedies only	GDPR damages; national laws	Civil claims; regulator-backed	State civil statutes; federal restitution	Civil penalties; eSafety scheme
Dedicated regulator for online harms	No (MeitY exercises executive functions)	Commission + national DSCs	Ofcom	FTC (for takedown regime)	eSafety Commissioner

Source. Compiled by the author from the official texts of the instruments cited (legislation.gov.uk; legislation.gov.au; congress.gov; EUR-Lex; Gazette of India) as in force on the date of writing.

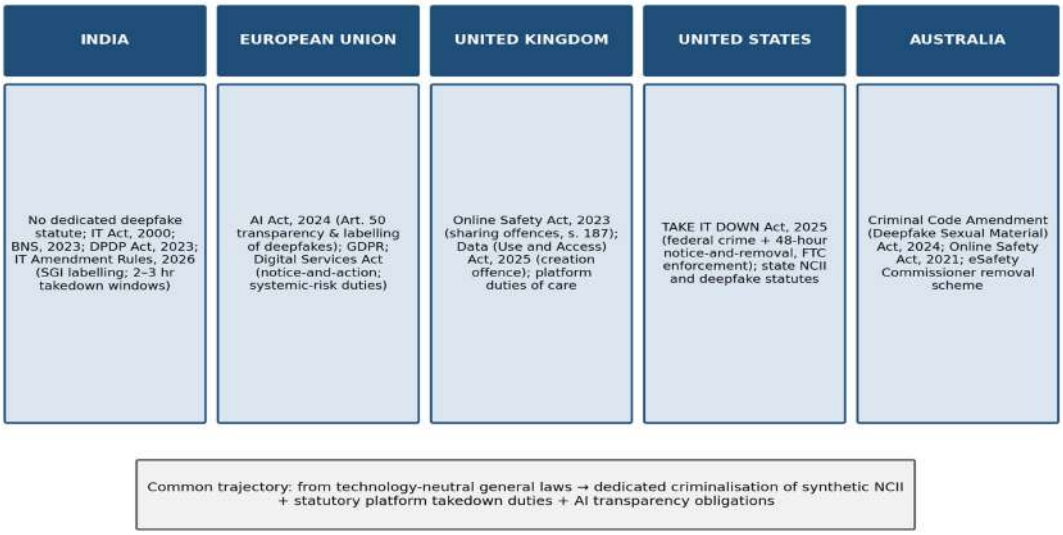

Figure-4: Comparative regulatory architectures for deepfake abuse.

14. Challenges in Investigation, Prosecution, and Evidence

14.1. Investigation

Deepfake investigations confront anonymity and extraterritoriality at every stage. Perpetrators operate behind pseudonymous accounts, virtual private networks, and encrypted channels; generation services and hosting infrastructure are frequently located abroad; and India's non-membership of the Budapest Convention leaves cross-border evidence gathering dependent on bilateral mutual legal assistance treaties, whose timelines are notoriously incompatible with the volatility of electronic evidence. Domestically, first-response capacity is uneven: complaints are routed through police cyber cells and the National Cybercrime Reporting Portal, but registration of a first information report for offences not squarely named in statute requires legal characterisation that station-level officers may be ill-equipped to perform, contributing to under-registration. The facts of *Mrs X* itself—where the victim's complaints to platforms and to the portal went unremedied until the High Court intervened—illustrate the gap between formal channels and effective response. The gendered dimension compounds this: the stigma attached to sexualised imagery deters many women from approaching police at all, a pattern extensively documented in the image-based sexual abuse literature **(Henry & Powell, 2018; McGlynn, Rackley, & Houghton, 2017)**.

14.2. Prosecution

Prosecutors must retrofit deepfake conduct into offences with ill-fitting ingredients: obscenity provisions that ignore consent; voyeurism provisions premised on a real private act; forgery provisions requiring characterisation of a synthetic video as a false electronic record made with requisite intent. Charge-stacking across the IT Act and BNS invites definitional challenges and inconsistent judicial outcomes, and the absence of reported appellate authority on synthetic imagery leaves trial courts without guidance. Sentencing provisions calibrated to obscenity, moreover, fail to reflect the sexual-violence character of the harm.

14.3. Evidence and Digital Forensics

The evidentiary core of a deepfake prosecution is proof of synthesis and attribution of authorship, both of which strain current forensic capacity. Detection is an adversarial moving target: survey literature documents that as detection models learn artefact signatures, generation models are trained to eliminate them **(Mirsky & Lee, 2021)**. Certification requirements for electronic records under Section 63 of the BSA discipline the chain of custody but do not resolve authentication of content; expert testimony on synthetic-media analysis remains scarce relative to the caseload of forensic science laboratories across digital-evidence categories. Conversely, deepfakes generate a systemic evidentiary externality that scholars term the "liar's dividend": as fabrication becomes plausible, genuine recordings can be disclaimed as fake, degrading the probative value of audio-visual evidence generally **(Chesney & Citron, 2019)**.

14.4. Platform Liability and Safe Harbour

Section 79 safe harbour, as construed in *Shreya Singhal*, protects intermediaries until actual knowledge through court or government channels—a construction protective of speech but slow for victims, and one that *Mrs X* already qualified by making strict compliance with the Rule 3 timelines a condition of the protection. The 2026 Amendment Rules invert the pressure: compressed timelines and verification duties, backed by loss of safe harbour, incentivise rapid and proactive removal, including through automated tools. The unresolved difficulty is calibration. Automated classifiers cannot reliably distinguish unlawful synthetic NCII from lawful expression at a two-to-three-hour cadence and at Indian scale, and the rational platform response to liability risk is over-removal **(van der Sloot & Wagensveld, 2022; Romero Moreno, 2024)**. The constitutional and policy challenge is to preserve the victim-protective speed of the new regime for the narrow category of intimate imagery while restoring procedural safeguards—reasoned orders, review, and transparency reporting—for contested categories of content.

15. Critical Analysis: Adequacy of the Framework and Legal Gaps

Measured against the evaluative criteria derived in Section 2—correct characterisation of the wrong, effective victim remedy, constitutionally disciplined platform power, and proportionality—and against the comparative baseline of Section 13, the Indian framework is best characterised as reactive, platform-centric, and perpetrator-lenient. Its principal deficiencies are consolidated in Table 5. First, and most fundamentally, no statute defines or criminalises the creation, solicitation, or distribution of non-consensual synthetic intimate imagery; every prosecution is an exercise in analogy. Second, the framework's centre of gravity is subordinate legislation—the 2026 Amendment Rules—whose obligations, however salutary, are of contestable vires, offer no remedy against perpetrators, and can be varied by executive action without parliamentary deliberation. The draft Second Amendment Rules noted in Section 10.2, which would make compliance with ministerial advisories and codes of practice a condition of safe harbour, illustrate the trajectory: were they notified, the content of intermediaries' legal obligations could be altered by executive instrument without even the formality of rule-making, a design in tension with the requirement of legality that *Puttaswamy* (2019) places at the threshold of any proportionality inquiry. Third, the victim's remedial position is weak: the DPDP Act channels penalties to the state rather than compensation to the victim; no statutory scheme provides interim relief, identity protection, or funded psychological support; and civil personality-rights remedies of the *Anil Kapoor* type are realistically available only to litigants of means.

Fourth, the consent-based wrong is misdescribed by obscenity-based offences, with expressive costs for victims and doctrinal costs for proportionality analysis. Fifth, institutional capacity—police cyber cells, forensic laboratories, prosecutorial expertise, and a dedicated online-safety regulator—lags the sophistication of the conduct. Sixth, ongoing policy processes remain unfinished: the long-signalled comprehensive replacement of the IT Act (publicly discussed since 2023 as a proposed "Digital India Act") had not been introduced in Parliament at the time of writing and must be treated as a policy proposal rather than law.

Table-5: Principal Legal Gaps in the Indian Framework

Gap	Description	Consequence for Women Victims
No dedicated offence	Neither the IT Act nor the BNS names non-consensual synthetic intimate imagery as an offence; creation per se is unpunished	Prosecutions rest on ill-fitting analogies; deterrence is weak; charge framing is inconsistent
Consent not an ingredient of content offences	Ss. 67/67A IT Act and s. 294 BNS are obscenity offences protecting public morality	The sexual-autonomy violation is legally invisible; victims risk definitional entanglement
Regulation by subordinate legislation	SGI regime created by executive rules under s. 87 IT Act, not by Parliament	Vires uncertainty; no perpetrator liability; obligations alterable without legislative scrutiny
No statutory victim remedy	DPDP penalties flow to the state; no compensation, interim-relief, or support scheme	Effective remedies confined to well-resourced civil litigants
Forensic and institutional deficit	Limited synthetic-media forensic capacity; no dedicated online-safety regulator	Delayed authentication, weak attribution, low conviction prospects
Cross-border enforcement gap	Non-membership of the Budapest Convention; MLAT delays	Foreign-hosted content and offenders effectively beyond reach

Over-removal risk	Hours-long takedown mandates enforced by safe-harbour forfeiture	Speech-protective safeguards of Shreya Singhal placed under strain; legitimacy of regime contestable

Source. Author's doctrinal analysis of the instruments and judgments cited in Sections 10 to 14.

16. Recommendations

The following reforms are proposed as a coherent legislative and institutional package, sequenced by priority into immediate reforms (0–1 year), medium-term reforms (1–3 years), and long-term reforms (3–5 years), and consolidated in Table 6 so that the agenda can be read directly as a policy roadmap. They are framed to survive Article 19 scrutiny by targeting the narrow, constitutionally unprotected core of the harm—non-consensual intimate depiction of identifiable persons—while regulating the wider synthetic-media ecosystem through transparency rather than prohibition.

16.1. Immediate Reforms (0–1 Year)

First, Parliament should enact a dedicated offence of non-consensual intimate imagery covering both authentic and synthetic depictions, on the pattern of the UK and Australian statutes: separate offences of (i) creating or soliciting the creation of, and (ii) publishing, transmitting, or threatening to publish, an intimate or sexual depiction—including a depiction created or altered by any technological means so as to appear to be of an identifiable person—without that person's consent, with aggravated penalties for creators-distributors, repeat offenders, and offences against minors (which must remain governed by the stricter child-protection regime). The offence should be gender-informed in design but drafted in gender-inclusive terms, define consent affirmatively, exclude motive requirements, and carry exemptions for law-enforcement, medical, judicial, and legitimate scientific purposes analogous to those in the TAKE IT DOWN Act. This is the single reform on which all others depend, because it names the wrong. Second, and simultaneously, the DPDP Act should be amended to restore an individual compensation remedy and to clarify that public availability of a photograph is not consent to its processing for sexualised synthesis—a targeted amendment achievable within the same legislative session.

16.2. Medium-Term Reforms (1–3 Years)

Third, the takedown regime for synthetic NCII should be placed on a statutory footing, converting the two-hour rule of the 2026 Amendment Rules into a parliamentary scheme with a victim-initiated notice mechanism, hash-matching obligations to prevent re-upload (generalising the *Mrs X* directions), protection for good-faith removal, and an independent appellate check—administered by a dedicated statutory online-safety authority modelled on Australia's eSafety Commissioner, with power to order de-indexing and to proceed against recalcitrant foreign services. Fourth, a statutory victim-remedy architecture should be created in the same instrument: a civil cause of action for compensation against creators and knowing distributors; power in the trial court to order interim takedown, preservation of evidence, and anonymisation of the victim in proceedings; restitution on conviction; and integration of NCII victims into victim-compensation schemes administered under the BNSS.

16.3. Long-Term Reforms (3–5 Years)

Fifth, capacity and cooperation measures require sustained investment: specialised synthetic-media units in state forensic science laboratories and the Indian Cyber Crime Coordination Centre; standard operating procedures and mandatory training for police on NCII complaints, including sensitivity protocols; judicial academy modules on the BSA's electronic-evidence regime as applied to synthetic media; and a reasoned reassessment of India's position on accession to the Budapest Convention or, at minimum, expanded bilateral arrangements for expedited preservation and disclosure of electronic evidence. Sixth, ecosystem-level AI governance should be consolidated in the comprehensive digital legislation that has been under public discussion as a successor to the IT Act: statutory transparency duties on providers of generative systems (provenance watermarking and

metadata, consistent with the 2026 labelling rules and Article 50 of the EU AI Act); a prohibition, enforced at the application-store and payment layers, on services whose principal function is the generation of sexualised imagery of identifiable persons without consent; and safe-harbour recalibration that preserves *Shreya Singhal*'s procedural safeguards for contested speech while retaining strict, fast-track duties for the narrow NCII category.

Table-6: Suggested Reforms, Prioritisation, and Rationale

Priority	Reform	Instrument	Comparative Anchor	Rationale
Immediate (0–1 yr)	Dedicated NCII offence (creation + solicitation + distribution; authentic + synthetic)	Amendment to BNS / new statute	UK OSA 2023 & DUAA 2025, s. 138; Australia 2024 Act; US TAKE IT DOWN Act	Names the wrong as sexual abuse; centres consent; cures analogical prosecution
Immediate (0–1 yr)	DPDP amendment: individual compensation; no "public data" consent inference for sexual synthesis	DPDP Act amendment	GDPR damages model	Restores the remedy lost with s. 43A IT Act; closes scraping loophole
Medium (1–3 yrs)	Statutory victim-initiated takedown + online-safety regulator + re-upload prevention	Parliamentary legislation replacing rule-based scheme	Australia eSafety; US 48-hr FTC scheme; EU DSA	Legal certainty and vires; appellate safeguards; systematises Mrs X directions
Medium (1–3 yrs)	Civil compensation, interim relief, anonymity, restitution for victims	Same statute + BNSS victim-compensation integration	US state civil statutes; UK regulator-backed claims	Shifts framework from platform-centric to victim-centred
Long (3–5 yrs)	Forensic and police capacity; judicial training; international cooperation review	Executive and budgetary measures; treaty policy review	Budapest Convention procedural model	Attribution and authentication are the operational bottleneck
Long (3–5 yrs)	Generative-AI transparency and design duties in comprehensive digital legislation	Successor legislation to the IT Act (currently policy debate)	EU AI Act Art. 50; India's SGI labelling rules (G.S.R. 120(E))	Prevention upstream; preserves lawful expressive uses

Source. Author's proposals, sequenced by legislative feasibility and dependence; comparative anchors as cited in Section 13.

17. Limitations of the Study

The findings must be read within the limits of the method. First, this is doctrinal research: it evaluates the law as enacted, notified, and judicially interpreted, and cannot measure how the framework operates in police stations, forensic laboratories, and trial courts; conclusions about enforcement are inferences from the design of the law and from reported decisions, not from field observation. Second, no interviews were conducted with victims, investigators, prosecutors, judges, or platform personnel, and no victim survey was undertaken; the lived experience of Indian deepfake victims is represented here only through reported judgments such as *Mrs X* and through foreign empirical literature whose samples rarely include South Asian populations. Third, the study depends on currently available reported judgments; because trial-court decisions in India are unevenly reported and appellate authority on synthetic imagery does not yet exist, the judicial picture presented may understate (or overstate) prosecutorial practice. Fourth, the quantitative context relies on NCRB administrative data, which measures registered rather than actual crime, does not disaggregate deepfake offences, and was available only up to the 2023 reporting year at the time of writing. Finally, the regulatory landscape analysed here is exceptionally fast-moving: the 2026 Amendment Rules may be judicially reviewed, the DPDP regime is in phased implementation, and comparative statutes are in early enforcement, so the analysis is expressly time-stamped and its comparative conclusions provisional. These limitations chart the agenda for future work: empirical studies of complaint-to-conviction attrition in Indian NCII cases, victim-centred qualitative research, and post-implementation review of the SGI regime.

18. Conclusion

Deepfake abuse of women is not a futuristic hypothesis but the dominant, empirically documented use of synthetic-media technology **(Ajder et al., 2019; Umbach et al., 2024)**, and it strikes at interests—privacy, dignity, sexual autonomy, and equal participation in public life—that Indian constitutional law ranks among its highest values. This article has shown that India's response, though accelerating, remains structurally incomplete. The Information Technology Amendment Rules, 2026 (G.S.R. 120(E)) give India a demanding platform regime for synthetic content, including a two-hour removal window for synthetic intimate imagery that is, on the comparative record examined here, among the shortest mandated anywhere, together with labelling and provenance duties that only the EU's AI Act otherwise approximates; the BNS, BNSS, and BSA modernise the general criminal apparatus; and the constitutional jurisprudence from *Puttaswamy* through *Subramanian Swamy*, *Navtej Singh Johar*, and *Kaushal Kishor* supplies a principled foundation extending to private-actor harms.

Yet the framework still contains no offence that names the harm, no remedy that reaches the victim, and no institution designed for the problem—and what regulation exists rests on subordinate legislation rather than parliamentary enactment. The comparative record—the United Kingdom, the United States, Australia, and the European Union all legislated dedicated offences and victim-facing mechanisms between 2023 and 2025—demonstrates that narrowly drawn, consent-centred legislation is both feasible and increasingly the international norm. The task for the Indian Parliament is to complete the architecture in the prioritised sequence proposed above: to criminalise non-consensual synthetic intimate imagery as sexual abuse, to convert executive takedown rules into statutory rights, to compensate and protect victims, and to do so with the drafting discipline that *Shreya Singhal* demands. Until it does, the law will continue to ask women to assemble justice from fragments.

The article's contribution to legal scholarship is threefold. Substantively, it offers the first doctrinal evaluation of deepfake abuse against the post-2024 Indian criminal architecture and the Information Technology Amendment Rules, 2026, verified against the Gazette texts, thereby updating a literature whose Indian analysis rests on repealed codes and superseded rules. Analytically, it positions India for the first time within the comparative matrix of the UK, US, Australian, and EU synthetic-imagery regimes, and applies an

explicit theoretical framework—feminist legal theory joined to informational privacy and digital constitutionalism—to generate evaluative criteria rather than description; the resulting diagnosis, that India has built platform accountability without perpetrator liability or victim remedy, is a structural claim testable against future enactments. Prescriptively, it converts that diagnosis into a time-sequenced legislative roadmap drafted to survive Article 19 scrutiny. Beyond the immediate Indian question, the analysis speaks to the future of AI governance generally: India's SGI regime is an early natural experiment in mandated provenance and rapid takedown, and its successes and pathologies—including the over-removal risk identified here—will inform how constitutional democracies discipline synthetic media while preserving the expressive freedoms that make that discipline legitimate.

Conflict of Interest

The authors declare no conflicts of interest.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration of Artificial Intelligence (AI) Assistance

Artificial intelligence tools were used only for grammar and language checking. The study design, data analysis, interpretation, and conclusions are entirely the work of the authors.

References

[1] Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). The state of deepfakes: Landscape, threats, and impact. Deeptrace.

[2] Amitabh Bachchan v. Rajat Nagi & Ors., CS(COMM) 819/2022 (Delhi High Court, 25 November 2022).

[3] Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi High Court, 20 September 2023).

[4] Arijit Singh v. Codible Ventures LLP & Ors. (Bombay High Court, interim order dated 26 July 2024).

[5] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India). https://www.indiacode.nic.in/

[6] Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India). https://www.indiacode.nic.in/

[7] Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India). https://www.indiacode.nic.in/

[8] Chaitanya Rohilla v. Union of India & Ors., W.P.(C) 15596/2023 (Delhi High Court).

[9] Chesney, B., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

[10] Citron, D. K. (2019). Sexual privacy. Yale Law Journal, 128(7), 1870–1960.

[11] Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. Wake Forest Law Review, 49(2), 345–391.

[12] Committee on the Elimination of Discrimination against Women. (1992). General Recommendation No. 19: Violence against women. United Nations.

[13] Committee on the Elimination of Discrimination against Women. (2017). General Recommendation No. 35 on gender-based violence against women, updating General Recommendation No. 19 (CEDAW/C/GC/35). United Nations.

[14] Congressional Research Service. (2025). The TAKE IT DOWN Act: A federal law prohibiting the nonconsensual publication of intimate images (LSB11314). Library of Congress. https://www.congress.gov/crs-product/LSB11314

[15] Constitution of India, 1950 (India). https://www.indiacode.nic.in/

[16] Convention on the Elimination of All Forms of Discrimination against Women, 18 December 1979, 1249 U.N.T.S. 13.

[17] Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Budapest.

[18] Criminal Code Amendment (Deepfake Sexual Material) Act 2024 (Cth) (Australia). https://www.legislation.gov.au/

[19] Data (Use and Access) Act 2025, c. 18 (United Kingdom). https://www.legislation.gov.uk/ukpga/2025/18

[20] Data (Use and Access) Act 2025 (Commencement No. 5) Regulations 2026, S.I. 2026/31 (United Kingdom). https://www.legislation.gov.uk/uksi/2026/31

[21] De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. International Journal of Constitutional Law, 19(1), 41–70. https://doi.org/10.1093/icon/moab001

[22] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India). https://www.indiacode.nic.in/

[23] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. Official Journal of the European Union, L series.

[24] Flynn, A., Powell, A., Scott, A. J., & Cama, E. (2022). Deepfakes and digitally altered imagery abuse: A cross-country exploration of an emerging form of image-based sexual abuse. British Journal of Criminology, 62(6), 1341–1358. https://doi.org/10.1093/bjc/azab111

[25] Gieseke, A. P. (2020). "The new weapon of choice": Law's current inability to properly address deepfake pornography. Vanderbilt Law Review, 73(5), 1479–1515.

[26] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27, 2672–2680.

[27] Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195–208. https://doi.org/10.1177/1524838016650189

[28] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India). https://www.indiacode.nic.in/

[29] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India, Extraordinary, Pt. II, s. 3(i) (25 February 2021), as amended by G.S.R. 794(E) (28 October 2022), G.S.R. 275(E) (6 April 2023), G.S.R. 775(E) (22 October 2025), and G.S.R. 120(E) (10 February 2026) (India).

[30] Jaikishan Kakubhai Saraf alias Jackie Shroff v. The Peppy Store & Ors., CS(COMM) 389/2024 (Delhi High Court, 2024).

[31] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

[32] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (Supreme Court of India).

[33] Kaushal Kishor v. State of Uttar Pradesh, (2023) 4 SCC 1 (Supreme Court of India).

[34] Kirchengast, T. (2020). Deepfakes and image manipulation: Criminalisation and control. Information & Communications Technology Law, 29(3), 308–323. https://doi.org/10.1080/13600834.2020.1794615

[35] Maddocks, S. (2020). 'A deepfake porn plot intended to silence me': Exploring continuities between pornographic and 'political' deep fakes. Porn Studies, 7(4), 415–423. https://doi.org/10.1080/23268743.2020.1757499

[36] Mania, K. (2024). Legal protection of revenge and deepfake porn victims in the European Union: Findings from a comparative legal study. Trauma, Violence, & Abuse, 25(1), 117–129. https://doi.org/10.1177/15248380221143772

[37] McGlynn, C., & Rackley, E. (2017). Image-based sexual abuse. Oxford Journal of Legal Studies, 37(3), 534–561. https://doi.org/10.1093/ojls/gqw033

[38] McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. Feminist Legal Studies, 25(1), 25–46. https://doi.org/10.1007/s10691-017-9343-2

[39] Meskys, E., Liaudanskas, A., Kalpokienė, J., & Jurcys, P. (2020). Regulating deep fakes: Legal and ethical considerations. Journal of Intellectual Property Law & Practice, 15(1), 24–31. https://doi.org/10.1093/jiplp/jpz167

[40] Ministry of Electronics and Information Technology. (2023). Advisories to intermediaries regarding misinformation, impersonation and deepfakes (7 November

2023 and 26 December 2023). Government of India.

[41] Ministry of Electronics and Information Technology. (2026a). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Gazette of India, Extraordinary, Pt. II, s. 3(i) (10 February 2026). Government of India. https://www.meity.gov.in/

[42] Ministry of Electronics and Information Technology. (2026b). Frequently asked questions on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. Government of India. https://www.meity.gov.in/

[43] Ministry of Electronics and Information Technology. (2026c). Draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Second Amendment Rules, 2026 [Draft notification, F. No. 2(5)/2025-CyberLaws, March 2026; not notified at the time of writing]. Government of India. https://www.meity.gov.in/

[44] Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. ACM Computing Surveys, 54(1), Article 7, 1–41. https://doi.org/10.1145/3425780

[45] Mrs X v. Union of India & Ors., 2023 SCC OnLine Del 2361 (Delhi High Court, 26 April 2023).

[46] National Crime Records Bureau. (2020). Crime in India 2019. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/

[47] National Crime Records Bureau. (2021). Crime in India 2020. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/

[48] National Crime Records Bureau. (2022). Crime in India 2021. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/

[49] National Crime Records Bureau. (2023). Crime in India 2022. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/

[50] National Crime Records Bureau. (2025). Crime in India 2023. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/

[51] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1 (Supreme Court of India).

[52] Öhman, C. (2020). Introducing the pervert's dilemma: A contribution to the critique of deepfake pornography. Ethics and Information Technology, 22(2), 133–140. https://doi.org/10.1007/s10676-019-09522-1

[53] Online Safety Act 2021 (Cth) (Australia). https://www.legislation.gov.au/

[54] Online Safety Act 2023, c. 50 (United Kingdom). https://www.legislation.gov.uk/ukpga/2023/50

[55] Press Information Bureau. (2024). MeitY advisory on due diligence by intermediaries and platforms concerning artificial-intelligence models (March 2024). Government of India. https://pib.gov.in/

[56] Rajat Sharma v. Union of India & Anr., W.P.(C) 6560/2024 (Delhi High Court).

[57] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). Official Journal of the European Union, L 277.

[58] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L series.

[59] Romero Moreno, F. (2024). Generative AI and deepfakes: A human rights approach to tackling harmful content. International Review of Law, Computers & Technology. Advance online publication. https://doi.org/10.1080/13600869.2024.2324540

[60] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).

[61] State of West Bengal v. Animesh Boxi (Court of Sessions, West Bengal, 2018) (trial-court decision; cited for illustration, without precedential force).

[62] Subramanian Swamy v. Union of India, (2016) 7 SCC 221 (Supreme Court of India).

[63] TAKE IT DOWN Act, Pub. L. No. 119-12, S. 146, 119th Congress (2025) (United States). https://www.congress.gov/bill/119th-congress/senate-bill/146

[64] Umbach, R., Henry, N., Beard, G. F., & Berryessa, C. M. (2024). Non-consensual synthetic intimate imagery: Prevalence, attitudes, and knowledge in 10 countries. In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24). Association for Computing Machinery. https://doi.org/10.1145/3613904.3642382

[65] van der Sloot, B., & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. Computer Law & Security Review, 46, 105716. https://doi.org/10.1016/j.clsr.2022.105716

[66] Viola, M., & Voto, C. (2023). Designed to abuse? Deepfakes and the non-consensual diffusion of intimate images. Synthese, 201, Article 30. https://doi.org/10.1007/s11229-022-04012-2

[67] Vysakh K.G. v. Union of India (Kerala High Court), as discussed in Mrs X v. Union of India, 2023 SCC OnLine Del 2361.

[68] Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/1282

[69] Westin, A. F. (1967). Privacy and freedom. Atheneum.

Cite this article as: Nadeem Alam and Shakeel Ahmad., (2026). Artificial Intelligence-Generated Deepfake Crimes Against Women in India: Evaluating the Adequacy of the Existing Legal Framework and the Need for Legal Reforms. International Journal of Emerging Knowledge Studies. 5(6), pp. 1025–1051.
https://doi.org/10.70333/ijeks-05-07-002