Page: 1315-1346 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.56

DEEPFAKE TECHNOLOGY, CYBERSTALKING, AND ONLINE HARASSMENT- A GENDERED ANALYSIS OF CYBERCRIME AND VICTIM PROTECTION MECHANISMS IN INDIA

Aditi Singh Bhadauria[1] & Dr. Rajeev Kumar Singh[2]

I. ABSTRACT

This paper examines how artificial intelligence enabled deepfakes, cyberstalking, and online harassment operate as gendered cybercrimes in India and how existing victim protection mechanisms perform in practice. It maps the production and circulation pathways of synthetic audio visual content, the tactics of surveillance, impersonation, doxxing, and threats, and the platform dynamics that accelerate harm through anonymity, virality, and algorithmic reinforcement. Using a doctrinal and socio legal method, the study analyses constitutional protections of privacy, dignity, equality, and speech limits, and evaluates statutory responses under the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the post reform criminal law framework under the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023. It further assesses intermediary due diligence obligations and emerging judicial trends on injunctions, takedowns, and victim centric reasoning. The findings highlight recurring implementation gaps, including delayed FIR conversion, uneven cyber policing capacity, weak preservation and certification of electronic evidence, cross border attribution barriers, and inconsistent platform response to repeat uploads. The paper proposes a calibrated reform blueprint that strengthens evidence first investigation protocols, improves portal to FIR workflows, expands compensation and confidentiality safeguards, and aligns platform governance with proportionality and due process. It also identifies future research priorities on prevalence measurement, intersectional impacts, and

[1] LLB 3rd year (6th semester) Student at Amity Law School, Lucknow Campus (India). Email: aditi.bhadauriya@s.amity.edu
[2] Assistant Professor of Law (Sr. Grade), Amity Law School Lucknow (India). Email: rksingh2@lko.amity.edu

 (ISSN: 2583-7753)

efficacy of provenance and transparency standards. Comparative insights from the EU, UK, and Australia illustrate risk based platform duties, deepfake disclosure norms, and administrative takedown models, while cooperation tools inform cross border electronic evidence requests.

II. KEYWORDS

Deepfakes, cyberstalking, online harassment, victim protection mechanisms, intermediary liability.

III. INTRODUCTION

A. Background of Research

Artificial intelligence has moved from decision support to content creation. Generative models now produce synthetic images, audio, and video that appear authentic to ordinary viewers. Deepfakes exploit this shift. They allow identity substitution, voice cloning, and fabricated scenes with very low friction. This changes cybercrime because it makes "credibility" cheap. It also turns reputational sabotage into a scalable tool of coercion, especially through sexualised fabrications and impersonation. CERT-In has formally characterised deepfakes as a high-severity threat category and has issued countermeasure guidance, signalling that the risk now sits within India's core cyber safety agenda.[3]

India's threat context also reflects an expanding cybercrime surface. Smartphone penetration, always-on social platforms, and digital payments create more points of capture and misuse. The National Crime Records Bureau compiles cybercrime statistics annually in its Crime in India publication, which has become an institutional reference point for the scale and shifting typologies of cyber offences in the country. Even where

[3] CERT-In Advisory CIAD-2024-0060, Deepfakes: Threats and Countermeasures (Nov. 27, 2024), https://www.cert-in.org.in/s2cMainServlet?VLCODE=CIAD-2024-0060&pageid=PUBVLNOTES02 (last visited Mar. 4, 2026).

reporting remains incomplete, official compilation underscores that cybercrime has matured into a routine category of policing and prosecution, not an exceptional event.[4]

Institutional response has developed alongside this growth. The Indian Cybercrime Coordination Centre under the Ministry of Home Affairs provides a national coordination framework for law enforcement agencies to address cybercrime in a comprehensive manner. Within this ecosystem, the National Cyber Crime Reporting Portal offers a centralised reporting channel that supports complaints across categories, including offences that carry gendered impacts such as cyberstalking, intimate image abuse, and online threats. This reporting architecture matters for deepfake abuse because early reporting can preserve platform logs and initial upload traces before deletion and reupload cycles begin.[5]

Policy attention to deepfakes has sharpened after visible episodes of AI-misinformation and impersonation. MeitY has issued advisories to intermediaries emphasising compliance with the IT Rules, with specific reference to misinformation represented by deepfakes. This indicates a regulatory view that deepfakes are not only a criminal misuse problem. They are also an intermediary governance problem involving user notice, prompt action workflows, and risk containment. The advisory approach also reflects the present legal posture, which relies on existing cyber law powers rather than a single dedicated deepfake statute.[6]

The legal background for this research therefore sits at an intersection. Constitutional guarantees of privacy, dignity, equality, and speech discipline inform how State action and platform action must remain proportionate. Statutory frameworks under the IT Act,

[4] NAT'L CRIME RECS. BUREAU, MINISTRY OF HOME AFFS., GOV'T OF INDIA, CRIME IN INDIA 2022 (Vol. I) (2023), https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf (last visited Mar. 4, 2026).

[5] National Cybercrime Reporting Portal (NCRP) Under I4C, INDIAN CYBER CRIME COORDINATION CENTRE (Ministry of Home Affairs), https://i4c.mha.gov.in/ncrp.aspx (last visited Mar. 4, 2026).

[6] Press Information Bureau, Gov't of India, MeitY Issues Advisory to All Intermediaries to Comply with IT Rules and Take Actions on Deepfakes (Dec. 26, 2023), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542 (last visited Mar. 4, 2026).

and the newly consolidated criminal law architecture under Bharatiya Nyaya Sanhita, 2023 and Bharatiya Nagarik Suraksha Sanhita, 2023, provide offence and procedure pathways. Yet deepfake harms often outpace investigation speed, and electronic evidence requirements demand early technical discipline. This combination creates a practical research need. It requires mapping how technology-enabled gendered harms travel through institutions, and where victim protection mechanisms still fail in real time.[7]

B. Research Questions,

1. How do deepfakes, cyberstalking, and online harassment operate as gendered cybercrimes in India, and what distinct harms do they create for dignity, privacy, autonomy, reputation, and physical safety?
2. How effectively do the IT Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 address deepfake-enabled harassment, and where do doctrinal gaps or overlap-based enforcement failures arise in practice?
3. How do investigation and evidence rules under the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 shape outcomes in deepfake and cyberstalking cases, especially on preservation, attribution, and admissibility?
4. What intermediary duties and court-led remedial trends most meaningfully protect victims, and what reforms can strengthen victim-centric redress without chilling lawful speech?

C. Research Objectives

1. To map the threat ecosystem of deepfakes and cyberstalking as gendered harms, and to classify the principal modes of victimisation, escalation patterns, and real-world consequences.

[7] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023 (India).

2. To doctrinally analyse India's constitutional protections and statutory offence framework for synthetic media abuse, and to identify enforcement gaps, ambiguity, or under-inclusive provisions.
3. To assess institutional capacity in reporting, investigation, and electronic evidence handling, with focus on preservation, chain of custody, and cross-border data constraints.
4. To evaluate platform governance and judicial remedies, and to propose a coherent reform blueprint across law, policing, platforms, and courts with strong due process safeguards.

D. Research Methodology

This study adopts a doctrinal and socio-legal methodology. It conducts close reading and interpretive analysis of constitutional principles, the IT Act, 2000, the Digital Personal Data Protection Act, 2023, and the new criminal law codes, alongside selected Supreme Court and High Court decisions on privacy, equality, speech limits, intermediary liability, and online abuse remedies. It then applies a socio-legal lens to identify implementation realities, using policy documents, official advisories, institutional portals, and credible reports to trace how victims report, how police investigate, and how platforms respond in practice. The analysis triangulates doctrine with operational constraints such as attribution barriers, electronic evidence admissibility, and cross-border data access, and it uses this synthesis to develop focused, victim-centric recommendations that remain proportionate and speech-sensitive.

IV. CONCEPTUAL FOUNDATIONS AND GENDERED HARM FRAMEWORK

A. Artificial Intelligence, Deepfakes, and the Attention Economy

AI systems increasingly generate, edit, and recombine audio-visual material with minimal cost and high fidelity. Deepfakes form a subset of synthetic media that uses machine learning to fabricate or alter identity cues such as face, voice, posture, and

context. This capability disrupts ordinary consent logic. A person can lose control over likeness and reputation without ever participating in the underlying act. In Indian constitutional terms, this is not merely "image misuse". It is an intrusion into decisional autonomy and dignity. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 supports treating privacy as a condition of personhood, and that framing helps courts see non-consensual deepfakes as dignitary harm with real constitutional weight.[8]

The attention economy supplies the propulsion system for deepfake harm. Platforms compete for time and engagement. They rank and recommend content that triggers emotion. That architecture rewards humiliation, outrage, and sexualised voyeurism. Deepfakes, especially those targeting women, fit this incentive structure too neatly. They invite clicks and shares, then the algorithm scales the harm. The victim's social standing becomes the "fuel" for attention capture, and attackers treat reputational injury as a cheap tool of coercion. Tim Wu's account of attention as a traded commodity explains why deepfakes rarely remain private insults. They often become mass events, with cascading reputational and safety risks.[9]

Intermediary liability doctrine then becomes the gatekeeper between harm reduction and overreach. Indian law does not permit a platform to behave like a private censor without constitutional discipline. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 read down section 79 of the IT Act, 2000 by linking "actual knowledge" to a court order or lawful governmental direction, rather than informal private complaints. This approach matters because deepfake victims need fast response, yet broad or vague takedowns can also silence women's counter-speech, journalism, and survivor narratives. The doctrine forces a legality filter while still leaving space for targeted, rule-based platform duties.[10]

[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[9] TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS (Alfred A. Knopf 2016).
[10] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

B. Cyberstalking and Online Harassment: Typologies and Patterns

Cyberstalking and online harassment operate through patterns, repetition, and escalation. Typologies include persistent messaging, surveillance through spyware or account compromise, impersonation, doxxing, threats, non-consensual intimate image abuse including deepfake variants, and coordinated pile-ons. A gendered analysis shows how these tactics converge into coercive control. The attacker often aims to restrict mobility, reputation, and economic participation. The abuse rarely stays "online only". It spills into workplaces, campuses, and family spaces. UN Women's work on online and ICT-facilitated violence captures this continuity of harm and supports treating such conduct as a rights-violating continuum rather than isolated "offensive speech".[11]

Patterns also reflect infrastructure. Harassment scales because digital systems lower friction for repeat contact, identity spoofing, and rapid redistribution. Attackers exploit platform affordances such as anonymity, forwarding features, quote-tweets, and recommendation engines. They also exploit gaps in detection, especially when manipulated media looks authentic to human viewers. Policy literature notes that deepfakes have become easier to generate than to detect, which shifts the compliance burden toward transparency, provenance, and rapid redress mechanisms. That insight matters in India because legal remedies often move slower than virality, and victims need interim protection measures that fit the speed of networked abuse.[12]

C. Gendered Vulnerability, Power, and Intersectionality in Digital Spaces

Digital spaces do not erase hierarchy. They often reproduce it with speed and scale. Misogyny, caste stigma, communal targeting, and queerphobia all travel through

[11] U.N. Women, Brief: Online and ICT-Facilitated Violence Against Women and Girls During COVID-19 (Apr. 2020), https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2020/Brief-Online-and-ICT-facilitated-violence-against-women-and-girls-during-COVID-19-en.pdf (last visited Mar. 4, 2026).

[12] ORG. FOR ECON. CO-OP. & DEV., Policy Responses to False and Misleading Digital Content 27 (2022), https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/08/policy-responses-to-false-and-misleading-digital-content_598ca9a6/1104143e-en.pdf (last visited Mar. 4, 2026).

platform affordances. Therefore, deepfakes and cyberstalking do not operate as "neutral tech abuse". They operate as power enforcement. The attacker selects the target because the target already faces social penalties for visibility. Then the attacker uses "proof-like" content to harden stereotypes. This is why intersectionality matters in legal analysis. It explains how one incident becomes many harms, across family control, workplace discrimination, and police distrust. The Supreme Court's dignity-centred approach in *National Legal Services Authority v. Union of India*, (2014) 5 SCC 438 supports this perspective because it recognises that social exclusion and structural discrimination shape the lived impact of rights violations.[13]

Online abuse also exploits intimate domains. It targets sexuality, relationships, clothing, and speech. That is a deliberate tactic. It converts patriarchal norms into digital coercion. The injury intensifies for queer persons, trans persons, and gender non-conforming individuals because the abuser can threaten "outing", or fabricate intimate conduct through deepfakes. The Court's reasoning in *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1 offers a constitutional vocabulary for this. It treats sexual orientation and gender identity as integral to personality and self-determination. So when abusers weaponise identity online, they do not merely offend. They strike at the core of constitutional personhood.[14]

Power in digital spaces also flows through institutions. Platforms decide ranking. Employers decide credibility. Police decide whether they will even register a complaint. This makes vulnerability a governance outcome, not only a victim attribute. Further, gendered abuse often uses coordinated mobs, not one offender. That structure produces "silencing by volume". It pushes women and marginalised genders off public platforms. A human rights frame helps courts and policymakers treat this as a participation harm, tied to equality and free expression. The UN Special Rapporteur on violence against women, in her report on online violence against women and girls, describes how online

[13] National Legal Services Authority v. Union of India, (2014) 5 SCC 438 (India).
[14] Navtej Singh Johar v. Union of India, (2018) 10 SCC 1 (India).

abuse restricts women's public participation and therefore engages State duties of prevention, protection, and redress.[15]

D. Harm Mapping: Dignity, Autonomy, Privacy, Reputation, and Safety

Dignity forms the first axis of harm. Deepfake sexual content reduces a person into an object for consumption. It publicly re-writes consent. It invites ridicule and moral policing. This is why courts should treat such conduct as a dignitary assault, not just obscenity. Autonomy forms the second axis. The victim often changes speech, mobility, and work choices. The attacker aims for that. Indian constitutional law supports mapping both dignity and autonomy together. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 locates privacy in dignity and personal choice, and that provides a principled basis to treat synthetic sexual defamation as an autonomy injury, not merely reputational upset.[16]

Privacy harm in these cases is rarely limited to "exposure". It includes surveillance, contact harvesting, and doxxing. It also includes informational coercion, where the abuser threatens disclosure to force compliance. Here, privacy includes control over dissemination, not only secrecy. It also includes protection against unlawful attacks on honour. International law supports this dual framing. The UN Human Rights Committee's General Comment No. 16 on Article 17 of the ICCPR clarifies that privacy protection extends against unlawful attacks on honour and reputation, including those emanating from private persons, not only the State. That approach strengthens the argument for robust State action against cyberstalking ecosystems.[17]

Reputation harm has distinct legal salience in India. It triggers social exclusion quickly, especially for women in conservative contexts. Deepfakes manufacture a narrative that

[15] Special Rapporteur on Violence against Women, Its Causes and Consequences, Rep. on Online Violence Against Women and Girls From a Human Rights Perspective, U.N. Doc. A/HRC/38/47 (June 18, 2018), https://docs.un.org/en/A/HRC/38/47 (last visited Mar. 4, 2026).
[16] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[17] U.N. Human Rights Comm., General Comment No. 16: Article 17 (Right to Privacy), ¶ 1, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (Apr. 8, 1988), https://www.refworld.org/legal/general/hrc/1988/en/27539 (last visited Mar. 4, 2026).

"looks true", so rebuttal becomes almost impossible. The law already recognises reputation as part of life under Article 21. *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221 affirms this, and it also situates reputation within the constitutional balance between speech and restriction. In gendered cybercrime, this balance must remain careful. Yet the baseline point stands. Reputation loss can become a deprivation of liberty in practice, because it blocks employment, education, and safe mobility.[18]

V. THREAT LANDSCAPE AND MODUS OPERANDI

A. Deepfake Production, Distribution, and Amplification Pathways

Deepfake production now follows a predictable pipeline. Offenders collect reference material first. They scrape photos and reels from public profiles. They lift voice notes from WhatsApp forwards, podcasts, short videos. Then they train or fine-tune models to mimic face and voice. They also use "one-shot" tools that need very little data. This lowers entry barriers. It also widens offender profiles from technically skilled actors to casual abusers and profit-driven extortionists. Law enforcement has already flagged deepfakes as a rapidly usable criminal capability, not a distant threat.[19]

Distribution typically starts in low-friction spaces. Private channels, closed groups, disposable accounts. The offender tests the content in smaller circles to see reaction. Then they seed it into larger platforms through reuploads. They also use link shorteners and mirror pages. In sexualised deepfake abuse, offenders often combine the content with threats and demands, so the "distribution" itself becomes leverage. The pathway also shifts across platforms to defeat moderation, and it exploits the delay between first upload and detection. Indian enforcement practice therefore needs early-stage preservation, because the initial upload often contains the best metadata trail.[20]

---

[18] Subramanian Swamy v. Union of India, (2016) 7 SCC 221 (India).
[19] EUROPOL, INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2024 22–24 (2024), https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf (last visited Mar. 4, 2026).
[20] EUROPOL, FACING REALITY: LAW ENFORCEMENT AND THE CHALLENGE OF DEEPFAKES (2022), https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes (last visited Mar. 4, 2026).

B. Cyberstalking Techniques: Surveillance, Impersonation, Doxxing, and Threats

Cyberstalking usually begins with surveillance. Offenders track stories, check-ins, friend lists, and comment patterns. They correlate that with phone numbers leaked in data breaches, or shared in delivery apps and local directories. They may also install spyware through malicious links, fake job forms, or "account verification" tricks. The point is control. Surveillance produces predictive power. It allows the offender to appear "everywhere" and that creates fear, and sometimes compliance. UNODC's cybercrime education materials treat digital evidence and device ecosystems as extended crime scenes, and that framing fits stalking because the behaviour spans many apps and devices.[21]

Impersonation comes next. Offenders clone accounts. They create look-alike handles. They steal profile photos. They then message friends and colleagues as the victim. In deepfake-enabled impersonation, offenders add voice notes, synthetic calls, and fake video snippets. This confuses witnesses fast. It also contaminates evidence. The victim must prove a negative, which is hard. Indian criminal law and cyber law can address this through cheating, identity related offences, and sexually coloured harassment provisions depending on facts, but investigators must document the timeline carefully. Otherwise, defence will later argue "reasonable doubt" due to account spoofing.[22]

Doxxing and threats turn harassment into a safety crisis. Doxxing exposes address, family details, workplace location, Aadhaar-linked identifiers, or intimate images. Threats then weaponise that disclosure, often with deadlines and demands. The legal response cannot treat this as mere speech. It is intimidation, coercion, and sometimes extortion. It also triggers a duty of prompt protection. Under Indian constitutional doctrine, State agencies must act with due care where liberty and dignity face credible threat. Courts have

[21] U.N. OFF. ON DRUGS & CRIME, CYBERCRIME MODULE 6: HANDLING OF DIGITAL EVIDENCE (E4J Univ. Module Series), https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html (last visited Mar. 4, 2026).
[22] U.N. OFF. ON DRUGS & CRIME, CYBERCRIME MODULE 4: DIGITAL EVIDENCE (E4J Univ. Module Series), https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-4/key-issues/digital-evidence.html (last visited Mar. 4, 2026).

repeatedly treated dignity as part of life under Article 21, and that logic makes protective action legally defensible even before trial completes.[23]

C. Platform Dynamics: Anonymity, Virality, and Algorithmic Reinforcement

Anonymity reduces social cost. It also fragments accountability. Abusers rotate handles. They use VPNs and temporary numbers. They hide behind throwaway email addresses. Yet anonymity is not absolute. Platforms still hold IP logs, device identifiers, and account recovery trails. So the practical question becomes speed and process. If preservation delays, logs expire. If notices lack precision, platforms resist disclosure. Therefore, the platform governance problem is not only "remove the post". It is evidence retention, transparency, and timely response structures.[24]

Virality amplifies gendered harm through repetition. Every share restates the insult. Every repost becomes a fresh publication. In deepfakes, virality also creates "belief by volume". Viewers assume truth because they see the content in many places. Algorithmic recommender systems then reinforce the cycle because engagement signals drive ranking. OECD work on false and misleading digital content explains how platform incentives and recommender design can accelerate misinformation spread. That analysis transfers well to deepfakes, because synthetic media thrives in the same incentive environment.[25]

D. Evidentiary Challenges: Attribution, Metadata, and Cross-border Actors

Attribution is the central evidentiary friction point. The visible account is often not the real actor. Offenders use compromised devices, rented botnets, or shared admin panels.

---

[23] National Legal Services Authority v. Union of India, (2014) 5 SCC 438 (India).
[24] INT'L ASS'N OF PROSECUTORS, EVIDENCE GATHERING AND CRIMINAL PROSECUTION IN CYBERCRIME CASES 19–22 (2018), https://www.iap-association.org/getattachment/Resources/Publications/Evidence-Gathering-and-Criminal-Prosecution-in-Cybercrime-Cases/Evidence-Gathering-and-Criminal-Prosecution-in-Cybercrime-Cases.pdf (last visited Mar. 4, 2026).
[25] ORG. FOR ECON. CO-OP. & DEV., POLICY RESPONSES TO FALSE AND MISLEADING DIGITAL CONTENT 15–18 (2022), https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/08/policy-responses-to-false-and-misleading-digital-content_598ca9a6/1104143e-en.pdf (last visited Mar. 4, 2026).

They also outsource segments of the workflow, like face dataset curation or distribution. Each layer increases plausible deniability. So investigators must build attribution using multiple anchors, not one. They need device forensics, account recovery trails, payment records, and server logs. The law of electronic evidence therefore must integrate technical chain-of-custody discipline with courtroom admissibility standards.[26]

Metadata is both fragile and powerful. It can show creation time, upload time, device model, editing history, and sometimes geolocation, though that is often stripped by platforms. Screenshots alone are weak. Courts prefer authenticated electronic records, and India's evidentiary doctrine has long insisted on certification for computer outputs. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 reinforced the 65B certificate requirement under the old Evidence Act. The Bharatiya Sakshya Adhiniyam, 2023 now codifies a similar approach in section 63, which means investigators must plan certification early, not at the last minute.[27]

VI. INDIAN LEGAL FRAMEWORK AND JUDICIAL APPROACH

A. Constitutional Protections: Privacy, Dignity, Equality, and Free Speech Limits

Indian constitutional doctrine treats privacy as an enabling right. It protects decisional autonomy. It also shields personality and dignity from forced exposure. So non-consensual deepfake pornography, voice cloning, and coerced circulation of intimate content can implicate Article 21 in a direct manner. The Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 located privacy in dignity and self-determination, which fits deepfake harm because the abuse rewrites consent and identity in public.[28]

Equality analysis also matters because digital abuse rarely distributes evenly. Gender, caste, disability, and queer identity shape targeting and impact. So courts can read

[26] INT'L CRIMINAL POLICE ORG. (INTERPOL), GUIDE FOR CRIMINAL JUSTICE STATISTICS ON CYBERCRIME AND ELECTRONIC EVIDENCE 6–9 (2020), https://www.interpol.int/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf (last visited Mar. 4, 2026).
[27] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
[28] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

Articles 14 and 15 as demanding non-discriminatory protection and effective remedies. *National Legal Services Authority v. Union of India*, (2014) 5 SCC 438 supports a dignity based equality method and it helps frame online humiliation and forced outing as structural discrimination, not private quarrel.[29]

Freedom of speech limits require careful calibration. The Constitution protects expression under Article 19(1)(a), yet Article 19(2) permits restrictions for decency, defamation, and public order. Deepfake regulation sits inside this balance. Courts must avoid broad censorship, but they can still restrain speech that functions as sexualised fraud, intimidation, or reputational sabotage. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 is central here because it rejects vague speech offences, and it ties intermediary "actual knowledge" to lawful orders, which matters in takedowns for deepfake abuse.[30]

B. Statutory Offences and Liabilities: IT Act and Penal Provisions

The IT Act, 2000 provides a functional offence toolkit for deepfakes and harassment. Section 66C addresses identity theft. Section 66D covers cheating by personation using computer resources, which can fit voice-clone scams and synthetic endorsement fraud. Section 66E targets violation of privacy through capturing or transmitting private images. Sections 67 and 67A cover obscene and sexually explicit electronic publication, which often anchors prosecution in morphed or deepfake sexual content. Sections 72 and 72A address breach of confidentiality and privacy in defined contexts, and section 85 supports corporate liability where systemic negligence enables misuse.[31]

Penal provisions under the Bharatiya Nyaya Sanhita, 2023 strengthen the response where conduct contains sexual harassment, stalking, voyeurism, intimidation, or threats. Section 75 criminalises sexual harassment in defined forms. Section 77 addresses voyeurism and it can fit covert capture and malicious dissemination. Section 78 criminalises stalking and it explicitly includes monitoring a woman's use of electronic

[29] National Legal Services Authority v. Union of India, (2014) 5 SCC 438 (India).
[30] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[31] Information Technology Act, 2000, No. 21 of 2000 (India).

communication, so cyberstalking becomes legally visible as stalking, not merely messaging. These provisions align with gendered harm patterns because they treat repeated conduct and surveillance as core wrongdoing.[32]

Criminal procedure has shifted toward tech-mediated investigation. The Bharatiya Nagarik Suraksha Sanhita, 2023 expands formal recognition of digital processes. It also pushes transparency through audio-video recording in defined investigative steps, which can reduce later disputes about how police collected devices or obtained access. This matters for deepfake cases because defence often attacks process gaps, not only facts. BNSS therefore becomes a practical safeguard for victims, if police actually follow the new procedural discipline.[33]

C. Intermediary Responsibility and Due Diligence Obligations

Intermediary responsibility in India rests on the IT Act's safe harbour structure under section 79, and the due diligence architecture under the 2021 Rules. The doctrine aims for a balance. It protects platforms from automatic criminal exposure for user content, yet it allows liability when platforms ignore lawful directions or fail mandated diligence. Delhi High Court reasoning in *My Space Inc. v. Super Cassettes Industries Ltd.*, 2016 SCC OnLine Del 6382 helps explain this logic because it separates general awareness from specific knowledge, and it stresses notice precision in takedown practice.[34]

Due diligence has special significance in synthetic media abuse. Platforms control the distribution layer. They also hold logs and account identifiers needed for attribution. So compliance should not mean only "remove one link". It should include preservation, traceability, and repeat-upload mitigation, within lawful scope. Government advisories on deepfakes have explicitly reminded intermediaries of Rule 3(1)(b) obligations and the

[32] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India).
[33] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023 (India).
[34] My Space Inc. v. Super Cassettes Industries Ltd., 2016 SCC OnLine Del 6382 (India).

need for prompt action against AI-misinformation and deepfake harms, which indirectly shapes platform risk management even when litigation has not started.[35]

D. Selected Judicial Trends: Injunctions, Takedowns, and Victim-Centric Reasoning

Indian courts increasingly grant quick injunctive relief where online abuse targets identity, sexuality, or reputation, and where circulation risks irreparable harm. Delhi High Court records in civil suits now show claims that explicitly plead "AI-generated visuals" and "deepfake material" alongside morphed nude content, and courts have issued restraint and takedown directions against unknown actors and platform links. This pattern signals a pragmatic move. Courts treat synthetic sexual abuse as urgent harm, not as a slow trial issue.[36]

Personality-rights litigation has also become a pathway for deepfake containment. In *Jubin Nautiyal v. Jammable Limited & Ors.*, CS(COMM) (Delhi High Court, Feb. 2026), the Court recorded allegations involving generative AI, deepfakes, face morphing, and unauthorised digital avatars, and it granted ex parte restraint directions against identified defendants and John Does. This trend matters for victim protection because it uses civil procedure to cut circulation while criminal investigation continues. It also forces platforms and marketplaces to remove monetised misuse, not only obscene content.[37]

VII. VICTIM PROTECTION AND INSTITUTIONAL RESPONSE

A. Reporting Pathways: Cyber Crime Portal, FIR, and Jurisdiction Issues

The National Cyber Crime Reporting Portal gives a formal entry point for victims who cannot reach a police station safely or quickly. It allows reporting of cybercrimes with a specific pathway for women and children related complaints, and it generates an

[35] Press Information Bureau, Gov't of India, MeitY Issues Advisory to All Intermediaries to Comply with IT Rules and Take Actions on Deepfakes (Dec. 26, 2023), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542 (last visited Mar. 4, 2026).
[36] O-23, CS(COMM) (Delhi High Court July 18, 2025) (order noting "morphed images, AI-generated visuals, deepfake material" and granting restraint directions).
[37] Jubin Nautiyal v. Jammable Limited & Ors., CS(COMM) (Delhi High Court Feb. 2026).

acknowledgement number that can help with follow up and escalation. Victims should treat the portal as a first secure record of the incident, not merely as "online feedback", and they should preserve the acknowledgement and the complaint narrative exactly as filed.[38]

The same ecosystem also supports rapid reporting for financial cyber fraud through the national helpline 1930, and it links reporting to state nodal and grievance contacts. Even when the principal harm is sexualised deepfake abuse or cyberstalking, offenders often add extortion demands and payment links later. Early reporting helps stop transaction chains and also creates a stronger trail of intent and coercion.[39]

A police station cannot refuse to register an FIR when the information discloses a cognizable offence. This becomes critical in deepfake porn circulation, threats, stalking, and identity impersonation because victims often face reluctance, moral policing, or jurisdiction excuses. The Supreme Court in *Lalita Kumari v. Government of Uttar Pradesh*, (2014) 2 SCC 1 treated registration as mandatory where information discloses a cognizable offence, and this principle remains a practical weapon for victims and counsel during escalation.[40]

Jurisdiction disputes commonly arise because the victim sits in one State, the offender operates from another, and the platform server sits outside India. In stalking and harassment, the "place of consequence" matters, because the injury occurs where the victim receives threats, suffers reputational harm, or faces surveillance. Police should focus on the continuity of the course of conduct, and record the chain of events across dates and platforms. This approach reduces the risk of mechanical rejection, and it

[38] Filing a Complaint on National Cyber Crime Reporting Portal, NAT'L CYBER CRIME REPORTING PORTAL (Gov't of India), https://cybercrime.gov.in/Webform/Accept.aspx (last visited Mar. 4, 2026).
[39] Report Online Financial Fraud at the National Cybercrime Helpline Number 1930, NAT'L CYBER CRIME REPORTING PORTAL (Gov't of India), https://cybercrime.gov.in/webform/Crime_NodalGrivanceList.aspx (last visited Mar. 4, 2026).
[40] Lalita Kumari v. Gov't of Uttar Pradesh, (2014) 2 SCC 1 (India).

matches the modern cybercrime architecture that I4C designs for coordinated law enforcement response.[41]

B. Investigation and Digital Evidence Handling: Preservation and Chain of Custody

The first investigative priority is preservation. Deepfake videos disappear, reappear, and mutate. Account names change. Links break. So police must issue preservation requests quickly to platforms and service providers, and they must seize and image devices in a way that keeps integrity. Victims should also preserve what they can without contaminating the chain. They should keep original messages, URLs, timestamps, and device identifiers. They should avoid repeated forwarding because forwarding can strip context and create evidentiary noise. UNODC's digital evidence guidance treats this as the difference between a usable case file and a collapsed case file.[42]

Indian evidence law now demands disciplined handling of electronic records in court. Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 sets conditions for admissibility of electronic records produced as computer outputs, and it requires a certificate with prescribed particulars at each instance where the record is submitted. Investigators must plan certification early and identify the person competent to sign. Otherwise, trial courts may exclude central screenshots, call logs, or platform extracts.[43]

The Supreme Court also treats certificate compliance as a structural requirement for electronic evidence, and it has rejected casual approaches that rely on informal printouts. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 reinforced the certificate requirement and clarified procedural expectations. This jurisprudence matters

[41] National Cybercrime Reporting Portal (NCRP) Under I4C, INDIAN CYBER CRIME COORDINATION CENTRE (Ministry of Home Affairs), https://i4c.mha.gov.in/ncrp.aspx (last visited Mar. 4, 2026).
[42] U.N. OFF. ON DRUGS & CRIME, Cybercrime Module 6: Handling of Digital Evidence, https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html (last visited Mar. 4, 2026).
[43] Bharatiya Sakshya Adhiniyam, 2023, § 63 (India).

for deepfakes because defence strategy frequently attacks authenticity, editing, and manipulation, and the prosecution must lock the integrity chain from the first day itself.[44]

Chain of custody needs simple but rigorous steps. Police should record seizure memos with device condition, IMEI or serial numbers, and details of who handled the device at each stage. They should use write blockers, hashes, and forensic imaging when feasible. They should maintain separate working copies so that the original stays untouched. The objective is to show that the prosecution did not create or alter the material, and that it moved through a documented custody path. A comparative mapping document from BPRD on BSA and the earlier Evidence Act shows that lawmakers retained the electronic record admissibility logic, which signals that courts will continue to demand discipline, not relaxation.[45]

C. Remedies: Criminal Process, Compensation, Protection Orders, and Civil Relief

Criminal process remains the principal remedy for deepfake sexual abuse, stalking, impersonation, and threats. The IT Act, 2000 supports charges for identity theft, cheating by personation, privacy violation, and publication of obscene or sexually explicit content, depending on facts. This statutory framework lets police draft charges that reflect both the synthetic media aspect and the coercion aspect, rather than collapsing the harm into a single label like "obscenity".[46]

Bharatiya Nyaya Sanhita, 2023 provisions strengthen response for stalking, sexual harassment, voyeuristic abuse, intimidation, and related offences. The victim protection value here is practical. It allows police to register a coherent narrative of repeated conduct and surveillance, which is the signature feature of cyberstalking. It also permits courts to

[44] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
[45] Bureau of Police Research & Development, Comparison Summary BSA to IEA (Gov't of India), https://bprd.nic.in/uploads/pdf/Comparison%20Summary%20BSA%20to%20IEA.pdf (last visited Mar. 4, 2026).
[46] Information Technology Act, 2000, No. 21 of 2000 (India).

consider safety risk at the bail stage because threats and repeat conduct indicate continuing danger, not a one-time incident.[47]

Compensation is not an afterthought. It is a stabilisation tool, especially where harassment causes job loss, relocation, therapy costs, or device replacement. Section 396 of the Bharatiya Nagarik Suraksha Sanhita, 2023 provides for a victim compensation scheme through State funds for victims who suffer loss or injury and need support even when offenders remain unidentified. This becomes important in deepfake cases because offenders often operate anonymously, and conviction may take years.[48]

Protection and confidentiality orders matter because "secondary dissemination" can restart harm at any time. Courts have recognised the need to protect the identity and privacy of victims of sexual offences, and they have insisted that authorities avoid public disclosure. *Nipun Saxena v. Union of India*, (2019) 2 SCC 703 directed protective handling of victim identity in records and cautioned against public exposure. That reasoning extends naturally to deepfake sexual abuse because the public interest does not require naming, and disclosure often multiplies harm.[49]

Civil relief can work alongside criminal process. Victims can seek injunctions to restrain publication, compel takedowns, and block mirror links, and they can plead privacy, reputation, and personality harms. Civil courts can also order disclosure of basic account information and monetisation trails in suitable cases, subject to due process. This route matters where the victim needs immediate containment. It also matters where platforms remove one instance but not derivatives, and the victim needs a continuing restraint mechanism.[50]

[47] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India).
[48] Bharatiya Nagarik Suraksha Sanhita, 2023, § 396 (India).
[49] Nipun Saxena v. Union of India, (2019) 2 SCC 703 (India).
[50] Specific Relief Act, 1963, No. 47 of 1963 (India).

D. Support Systems: Legal Aid, Counselling, and Safety Planning

Victims often delay reporting because they fear stigma, retaliation, or police disbelief. Free legal aid can reduce this barrier. NALSA's legal aid framework under the Legal Services Authorities Act, 1987 provides institutional pathways for free services to eligible persons, including women, children, and other categories recognised by the statute and rules. For technology-facilitated sexual harassment, early legal counselling helps preserve evidence, draft accurate complaint narratives, and prevent accidental self-incrimination through reactive social media responses.[51]

Support systems must also include counselling and trauma-informed care. Deepfake sexual abuse and stalking create chronic fear, sleep disruption, and public shame. Counselling supports decision-making, and it reduces long-term harm. UN Women's work on online and ICT-facilitated violence explains how technology abuse affects mental health and participation in public life, and it supports the argument for integrated victim services rather than a police-only response model.[52]

Safety planning should operate as an immediate protocol, not a generic suggestion. Victims should lock accounts, enable two factor authentication, check for device compromise, and review privacy settings across platforms. They should document harassment patterns in a single log with dates, times, and URLs. They should inform one trusted person and set a check-in routine. Police should treat safety planning as part of victim assistance because threats often escalate after first reporting, not before. The cybercrime portal itself lists emergency and support helplines, including the national

[51] Legal Aid, NAT'L LEGAL SERVS. AUTH., https://nalsa.gov.in/legal-aid/ (last visited Mar. 4, 2026).
[52] U.N. Women, Brief: Online and ICT-Facilitated Violence Against Women and Girls During COVID-19, https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2020/Brief-Online-and-ICT-facilitated-violence-against-women-and-girls-during-COVID-19-en.pdf (last visited Mar. 4, 2026).

police helpline 112 and women helpline 181, which can be integrated into safety plans when risk spikes.[53]

VIII. COMPARATIVE AND POLICY PERSPECTIVES

The European Union has moved toward an "ex ante transparency" model for synthetic media. The EU's AI regulatory framework expects deployers and providers of certain AI systems to disclose that content is artificially generated or manipulated, including deepfakes, and to adopt marking or labelling mechanisms where appropriate. This approach treats disclosure as a governance baseline, not a discretionary platform policy. It aims to reduce belief by default, which deepfakes exploit. For India, the lesson is clear. A legal duty to signal synthetic origin can reduce harm even before takedown, especially where abuse spreads faster than enforcement. It also supports evidentiary integrity because provenance signals can help investigators trace creation and distribution pathways.[54]

The EU Digital Services Act illustrates a "systemic risk" approach for large platforms. It goes beyond individual notices. It expects very large online platforms to assess and mitigate systemic risks linked to illegal content, disinformation, and threats to fundamental rights, and it ties these expectations to transparency and accountability duties. This architecture matters for deepfakes and gendered harassment because the harm is not only the first upload. The harm is repeated exposure, recommendation loops, and cross-platform replication. India's intermediary framework already imposes due diligence duties, but comparative learning suggests a stronger shift from link-level takedown to risk-level prevention, including friction for reuploads and better reporting pathways for targeted abuse.[55]

---

[53] Cyber Crime Reporting Portal Conditions Page (Helplines 112, 181, 1930), NAT'L CYBER CRIME REPORTING PORTAL (Gov't of India), https://cybercrime.gov.in/Webform/crmcondi.aspx (last visited Mar. 4, 2026).

[54] AI Act, Shaping Europe's Digital Future (European Commission), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (last visited Mar. 4, 2026).

[55] The Digital Services Act, Shaping Europe's Digital Future (European Commission), https://digital-strategy.ec.europa.eu/en/policies/digital-services-act (last visited Mar. 4, 2026).

The United Kingdom's post-OSA policy direction foregrounds "safety by design" and explicitly places violence against women and girls within online safety priorities. This matters because it reframes online harassment as a public safety and equality issue, not a private dispute. It also strengthens the case for regulated transparency, with expected oversight of platform practices and measurable outcomes. For India, the policy lesson lies in institutional design. A victim-centric model works best when regulators can demand process data, response timelines, and escalation logs, rather than trusting informal compliance. It also helps India align cyber safety governance with constitutional equality, not only with criminal prohibition.[56]

Australia offers a distinctive victim-facing administrative model through the eSafety Commissioner, including a formal image-based abuse scheme that enables victims to seek removal of intimate images shared without consent. This model reduces dependency on slow criminal procedure for immediate containment. It also recognises that victims often need swift takedown and support even when perpetrators remain unknown or overseas. For India, this suggests a policy option worth serious study. A specialised statutory authority with removal and coordination powers can sit alongside police and courts. It can also standardise victim communications, reduce stigma at the first contact point, and improve reporting retention.[57]

IX. FINDINGS, RECOMMENDATIONS, AND CONCLUSION

A. Key Findings and Implementation Gaps

Deepfake-enabled abuse has shifted the harm curve. It combines sexualised falsification with rapid distribution. The victim faces forced "public proof" and coerced silence. This pattern fits the constitutional logic of privacy as decisional autonomy and dignity, not

[56] U.K. Dep't for Sci., Innovation & Tech., Statement of Strategic Priorities for Online Safety (Feb. 27, 2025), https://assets.publishing.service.gov.uk/media/6863afdd1c735341c2111b58/Final_Statement_of_Strategic_Priorities_for_Online_Safety.pdf (last visited Mar. 4, 2026).

[57] Current Legislation, Dep't of Infrastructure, Transp., Reg'l Dev., Commc'ns & the Arts (Austl.), https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation (last visited Mar. 4, 2026).

mere secrecy, so the harm is structural and rights-based. Yet practice still treats it as ordinary obscenity or "morphing", which under-describes the coercion and the identity capture.[58]

Reporting remains uneven. Victims often start on the National Cyber Crime Reporting Portal but struggle to convert complaints into timely FIRs, especially when police raise jurisdiction objections. This gap matters because deepfake links mutate quickly, and the first hours carry the best attribution trail. Under Indian law, police must register an FIR when information discloses a cognizable offence, but the ground reality still shows friction and delay.[59]

Investigation quality varies sharply across States and stations. Digital evidence handling still shows weak preservation habits. Many cases rely on screenshots and informal printouts. Defence then attacks authenticity and chain of custody. The new evidentiary regime expects structured certification and device particulars for electronic records, so casual collection now causes direct courtroom exclusion risk.[60]

Platform-side responsiveness remains inconsistent. Safe harbour doctrine protects intermediaries but it also expects compliance with due diligence and lawful takedown directions. However, victims still face slow removals, partial removals, or reupload cycles. This becomes an implementation gap, not a doctrinal gap. The State has already issued deepfake advisories to remind intermediaries of their obligations, which indicates that the government also sees compliance drift as a live issue.[61]

Victim support remains fragmented. Many victims need urgent stabilisation. They need counselling, privacy-preserving processes, and interim safety planning. The system still routes them through multiple desks. This increases drop-out. Victim compensation

[58] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
[59] Lalita Kumari v. Gov't of Uttar Pradesh, (2014) 2 SCC 1 (India).
[60] Bharatiya Sakshya Adhiniyam, 2023, § 63 (India).
[61] Press Information Bureau, Gov't of India, MeitY Issues Advisory to All Intermediaries to Comply with IT Rules and Take Actions on Deepfakes (Dec. 26, 2023), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542 (last visited Mar. 4, 2026).

frameworks exist, but awareness and access remain limited, especially when the offender stays unidentified or abroad.[62]

B. Reform Proposals: Law, Policing, Platforms, and Courts

Law reform should target clarity without overbreadth. India can retain the present offence basket under the IT Act and BNS, yet add a narrow synthetic sexual abuse offence or an aggravated form where a person fabricates intimate content using another's likeness without consent and circulates it with intent to harass, extort, or humiliate. Drafting must stay precise. It must not criminalise satire, parody, or bona fide journalism, and it must preserve Article 19(1)(a) discipline through clear mens rea and defences. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 provides the constitutional warning against vague speech-linked criminality.[63]

Policing reform should focus on first-response SOPs. Each cyber cell should use a standard "preserve-first" protocol. It should issue preservation notices to platforms within hours. It should seize devices with documented chain of custody. It should record hashes where feasible. It should also train IOs on identifying deepfake artefacts and on drafting platform requests with precise URLs, channel IDs, and timestamps. BNSS already embeds a more technology-enabled criminal procedure vision, and States should translate that vision into operational checklists and supervision.[64]

Platforms should carry enforceable duties on reupload mitigation for verified intimate abuse and deepfake sexual content. A notice-and-action model alone fails when the same file reappears in minutes. So due diligence should include repeat-hash blocking, friction on forwarding, and clearer user reporting flows, while still preserving lawful speech and appeal processes. Technical provenance and labelling can reduce "belief by default" and assist investigators, but compliance should stay proportionate and auditable. The IT

[62] Bharatiya Nagarik Suraksha Sanhita, 2023, § 396 (India).
[63] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[64] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023 (India).

Rules already operate as the due diligence spine for intermediaries, so this reform can be anchored in that delegated framework rather than a fresh statute.[65]

Courts can strengthen victim-centric relief through consistent interim orders. Civil injunctions should focus on rapid takedown, mirror-link restraint, and limited disclosure directions that enable attribution, subject to due process. Criminal courts can adopt a safety-first approach at bail where threats show ongoing danger. Courts can also push strict electronic evidence compliance early, so the prosecution does not attempt last-minute certification. The Supreme Court's approach in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 underlines that electronic evidence admissibility is not a casual formality.[66]

Compensation and protection should be treated as parallel remedies, not post-verdict add-ons. Section 396 of BNSS enables compensation even where the offender is not traced, which fits the reality of anonymous deepfake networks. Legal services authorities can also develop fast-track counselling and legal aid protocols for technology-facilitated sexual abuse, and courts should insist on privacy-preserving record handling to avoid secondary victimisation.[67]

C. Conclusion and Future Research Directions

Future research should measure prevalence and harm escalation in India using rigorous sampling, not only police FIR counts. It should map the gendered and intersectional distribution of targeting, including caste, disability, queer identity, and regional factors. It should also study how reputational harm translates into job loss, education disruption, and relocation, because these are the real liberty costs in practice. The Ministry of Home

[65] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[66] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
[67] Legal Services Authorities Act, 1987, No. 39 of 1987 (India).

Affairs reporting on cybercrime capacity and systems signals scale and growth, but it still needs granular research that captures non-reporting and drop-outs.[68]

Research should also test governance tools. Provenance standards, watermarking, and detection systems must be evaluated against adversarial adaptation. Comparative work can examine how systemic risk models and safety-by-design obligations influence platform behaviour, and what due process safeguards best prevent over-removal. Evidence-focused research should also develop practical templates for section 63 certification, preservation notices, and cross-border request formats, so police and prosecutors reduce failure rates in court. The UNODC cross-border electronic evidence guidance offers a structured baseline for such operational research.[69]

X. BIBLIOGRAPHY

A. Constitutional and Supreme Court Decisions

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
2. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).
3. *National Legal Services Authority v. Union of India*, (2014) 5 SCC 438 (India).
4. *Navtej Singh Johar v. Union of India*, (2018) 10 SCC 1 (India).
5. *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221 (India).
6. *Lalita Kumari v. Gov't of Uttar Pradesh*, (2014) 2 SCC 1 (India).
7. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
8. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
9. *Nipun Saxena v. Union of India*, (2019) 2 SCC 703 (India).

[68] Ministry of Home Affairs, Gov't of India, Annual Report 2023–24 (Dec. 27, 2024), https://xn--i1b5bzbybhfo5c8b4bxh.xn--11b7cb3a6a.xn--h2brj9c/sites/default/files/AnnualReport_27122024.pdf (last visited Mar. 4, 2026).
[69] U.N. Off. on Drugs & Crime, Practical Guide for Requesting Electronic Evidence Across Borders (2020), https://www.unodc.org/cld/en/publications/practical-guide/practical-guide.html (last visited Mar. 4, 2026).

10. *Aparna Bhat v. State of Madhya Pradesh*, 2021 SCC OnLine SC 230 (India).

11. *MySpace Inc. v. Super Cassettes Indus. Ltd.*, 2016 SCC OnLine Del 6382 (India).

12. Information Technology Act, 2000, No. 21 of 2000 (India).

13. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

14. Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023 (India).

15. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46 of 2023 (India).

16. Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023 (India).

17. Specific Relief Act, 1963, No. 47 of 1963 (India).

18. Legal Services Authorities Act, 1987, No. 39 of 1987 (India).

B. Indian Rules, Government Advisories, and Official Portals

1. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India) (as amended Feb. 10, 2026).

2. Frequently Asked Questions on IT Rules, 2021 Amendment (Synthetic-Generated Information Framework) (Feb. 10, 2026) (India), https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf (last visited Mar. 4, 2026).

3. Press Information Bureau, Gov't of India, MeitY Issues Advisory to All Intermediaries to Comply with IT Rules and Take Actions on Deepfakes (Dec. 26, 2023), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542 (last visited Mar. 4, 2026).

4. CERT-In Advisory CIAD-2024-0060, Deepfakes: Threats and Countermeasures (Nov. 27, 2024), https://www.cert-in.org.in/s2cMainServlet?VLCODE=CIAD-2024-0060&pageid=PUBVLNOTES02 (last visited Mar. 4, 2026).

5. National Cyber Crime Reporting Portal (Gov't of India), https://cybercrime.gov.in/ (last visited Mar. 4, 2026).

6. Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, https://i4c.mha.gov.in/ (last visited Mar. 4, 2026).

7. Ministry of Home Affairs, Gov't of India, Annual Report 2023–24, https://xn--i1b5bzbybhfo5c8b4bxh.xn--11b7cb3a6a.xn--h2brj9c/sites/default/files/AnnualReport_27122024.pdf (last visited Mar. 4, 2026).

C. Indian Official Statistics and Government Publications

1. Nat'l Crime Recs. Bureau, Ministry of Home Affs., Gov't of India, *Crime in India 2022* (2023), https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608543CrimeinIndia2022Book3.pdf (last visited Mar. 4, 2026).

2. Ministry of Electronics & Information Technology (MeitY), Digital Personal Data Protection Act, 2023 (official PDF), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited Mar. 4, 2026).

3. Ministry of Home Affairs, Bharatiya Nyaya Sanhita, 2023 (official PDF), https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (last visited Mar. 4, 2026).

4. Ministry of Home Affairs, Bharatiya Sakshya Adhiniyam, 2023 (official PDF), https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited Mar. 4, 2026).

D. International Instruments and UN Materials

1. International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

2. U.N. Human Rights Comm., General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (Apr. 8, 1988), https://www.refworld.org/legal/general/hrc/1988/en/27539 (last visited Mar. 4, 2026).

3. Special Rapporteur on Violence against Women, Its Causes and Consequences, Rep. on Online Violence Against Women and Girls From a Human Rights Perspective, U.N. Doc. A/HRC/38/47 (June 18, 2018), https://docs.un.org/en/A/HRC/38/47 (last visited Mar. 4, 2026).

4. U.N. Women, Brief: Online and ICT-Facilitated Violence Against Women and Girls During COVID-19 (Apr. 2020), https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2020/Brief-Online-and-ICT-facilitated-violence-against-women-and-girls-during-COVID-19-en.pdf (last visited Mar. 4, 2026).

E. Comparative Digital Regulation and Cybercrime Cooperation

1. Digital Services Act, Regulation (EU) 2022/2065, 2022 O.J. (L 277) 1.

2. European Commission, Digital Services Act, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act (last visited Mar. 4, 2026).

3. European Commission, AI Regulatory Framework (AI Act policy page), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (last visited Mar. 4, 2026).

4. Council of Europe, Budapest Convention on Cybercrime (Convention overview), https://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Mar. 4, 2026). (Portal)

5. Council of Europe, 24/7 Network Established Under the Convention on Cybercrime, https://www.coe.int/en/web/cybercrime/24/7-network-new (last visited Mar. 4, 2026).

6. U.K. Dep't for Sci., Innovation & Tech., Statement of Strategic Priorities for Online Safety (Feb. 27, 2025), https://assets.publishing.service.gov.uk/media/6863afdd1c735341c2111b58/Final_Statement_of_Strategic_Priorities_for_Online_Safety.pdf (last visited Mar. 4, 2026).

7. Dep't of Infrastructure, Transp., Reg'l Dev., Commc'ns & the Arts (Austl.), Current Legislation (Online Safety), https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation (last visited Mar. 4, 2026).

8. eSafety Commissioner (Austl.), Image-Based Abuse Scheme Regulatory Guidance (Feb. 2024), https://www.esafety.gov.au/sites/default/files/2024-02/Image-Based-Abuse-Scheme-Regulatory-Guidance-Feb2024.pdf (last visited Mar. 4, 2026).

F. Technical Standards, Cyber Policing Guides, and Research Reports

1. Nat'l Inst. of Standards & Tech., *Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency* (NIST AI 100-4, 2024), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-4.pdf (last visited Mar. 4, 2026).

2. Org. for Econ. Co-operation & Dev., *Policy Responses to False and Misleading Digital Content* (2022), https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/08/policy-responses-to-false-and-misleading-digital-content_598ca9a6/1104143e-en.pdf (last visited Mar. 4, 2026).

3. Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2024* (2024), https://www.europol.europa.eu/publications-events/publications/internet-organised-crime-threat-assessment-iocta-2024 (last visited Mar. 4, 2026).

4. Europol, *Facing Reality: Law Enforcement and the Challenge of Deepfakes* (2022), https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes (last visited Mar. 4, 2026).

5. U.N. Off. on Drugs & Crime, Cybercrime Module 6: Handling of Digital Evidence, https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html (last visited Mar. 4, 2026).

6. U.N. Off. on Drugs & Crime, *Practical Guide for Requesting Electronic Evidence Across Borders* (2020), https://www.unodc.org/cld/en/publications/practical-guide/practical-guide.html (last visited Mar. 4, 2026).

G. Scholarly Books and Monographs

1. Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (Alfred A. Knopf 2016).