DEEPFAKE ABUSE IN INDIA: A LEGAL VACUUM IN CRIMINAL LAW

Khushi Mokati, Student, Gujarat National Law University, Gandhinagar

ABSTRACT

The rapid spread of deepfake technology in India has revealed structural gaps in the country's criminal law system. Artificial intelligence-generated synthetic media now enables non-consensual sexual imagery, financial fraud, identity impersonation, political manipulation, and other harms that existing statutory provisions cannot adequately address. India's current legal response remains fragmented and reactive, relying on dispersed sections of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, neither of which accounts for the technical process or scale of deepfake production. The absence of a statutory definition of "deepfake," combined with jurisdictional difficulties, slow cross-border cooperation and limited forensic capacity create a regulatory vacuum that disproportionately affects women, children, and marginalised communities. This paper examines these systemic shortcomings through statutory analysis and recent case law, including Ankur Warikoo v. John Doe (2025) and Global Health Limited v. John Doe (2025). The analysis shows that while Indian courts have attempted to bridge these gaps through interim injunctions, takedown directions, and flexible readings of existing provisions, judicial innovation cannot function as a long-term substitute for coherent legislation. Drawing from comparative regulatory models in the European Union, United States, and China, the paper proposes a structured legislative framework grounded in consent-based protections, platform accountability, user verification duties, and enforceable cross-border mechanisms. It concludes that India requires anticipatory, technology-specific criminal legislation that balances innovation with constitutional rights, protects digital identity and personal dignity, and establishes clear obligations for creators, platforms, and regulators within the country's rapidly evolving digital ecosystem. The paper ultimately argues that India must harmonise its emerging digital laws with sector-specific regulations to prevent fragmentation and ensure coherent enforcement.

Key Words: *- Deepfakes in India, Synthetic Media Regulation, Digital Criminal Law, Platform Accountability, Consent-Based Protections*

I. INTRODUCTION

When actress Rashmika Mandanna's face appeared in an obscene video that went viral across social media in October 2023, it wasn't actually her. A young engineer running a fan page had used AI to superimpose her face onto British-Indian influencer Zara Patel's body, all done to boost Instagram followers.[1] Delhi Police arrested him in January 2024, after the video had already been viewed by millions and ignited a national debate on deepfakes.

Fast forward to 2025, and the problem has exploded. Personal finance educator Ankur Warikoo secured a landmark Delhi High Court injunction after deepfake videos of him promoting fraudulent stock market schemes circulated on WhatsApp.[2] Renowned cardiac surgeon Dr. Naresh Trehan obtained similar relief when deepfake videos showing him giving bogus medical advice went viral.[3]

The uncomfortable reality is that as deepfakes proliferate, India's criminal law remains reactive, fragmented, and structurally ill-equipped to address AI-generated identity abuse at scale. This paper argues that the absence of a consent-centred, technology-specific criminal framework has created a regulatory vacuum that courts cannot permanently fill.

II. THE REALITY CHECK: WHY SHOULD YOU CARE?

Globally, an overwhelming majority of deepfake content is sexually explicit, and nearly all victims are women.[4] In India, deepfakes have also become powerful tools for financial fraud. Impersonation scams have caused financial losses running into crores. What was once a niche technological threat has now become a mass-scale tool for exploitation.

The India Cyber Security Threat Report 2025 labels deepfake-enabled cybercrime as critical, predicting that malicious content from "trusted sources" will facilitate devastating social engineering attacks.

---

[1]"Did it to Get Instagram Followers: How Man Behind Rashmika Mandanna Deepfake Was Caught", Business Today, Jan. 21, 2024, available at: https://www.businesstoday.in/india/story/did-it-to-get-instagram-followers-how-man-behind-rashmika-mandanna-deepfake-was-caught-414295-2024-01-21 (last visited on Dec. 20, 2025).
[2]Ankur Warikoo v. John Doe, 2025 SCC OnLine Del 3727.
[3]Global Health Limited v. John Doe, CS(COMM) 6/2025 (Delhi High Court).
[4]Meenakshi Malik Sharma, "Deepfake Pornography: Impact on Women's Rights" International Journal for Multidisciplinary Research (2024).

III. THE DEEPFAKE PHENOMENON: SCALE AND IMPACT

A. Quantifying the Threat

Contrary to popular assumption, deepfake harm is not limited to public figures. India's high smartphone penetration (over 750 million users in 2024) increases exposure to deepfake abuse.[5] The dominance of social media platforms, particularly WhatsApp and Instagram, enables rapid content diffusion across linguistic and geographic boundaries.

In India, deepfakes have also become powerful tools for financial fraud. In June 2025, a 79-year-old woman in Bengaluru lost ₹35 lakhs to deepfaked videos of N.R. Narayana Murthy promoting fake investments.[6] Similar scams using the likeness of other public figures have resulted in losses running into crores. I4C data indicates over 740,000 cybercrime complaints in early 2024, averaging 7,000 per day.[7]The India Cyber Security Threat Report 2025 labels deepfake-enabled cybercrime as critical, predicting that malicious content from "trusted sources" will facilitate devastating social engineering attacks.[8] These numbers indicate that India's risk profile is rising faster than its legal response mechanisms.

B. Political Manipulation and Democratic Erosion

Beyond personal and financial harms, deepfakes also threaten democratic stability. One example involved a deepfake using a cloned voice of Mahatma Gandhi endorsing a political party.[9]In 2025, Fabricated videos during state elections prompted I4C intervention, highlighting risks to electoral integrity.[10]These incidents illustrate the 'liar's dividend,' where deepfakes enable

---

[5]Sommya Kashyap, "The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology" 22(2) SCRIPTed 162 (2025).

[6]"AI scam uses Narayana Murthy deepfake, dupes 79-year-old Bengaluru woman of Rs 35L; fake UK firm ran 'trading platform'; cops probing extortion angle", The Times of India, available at: https://timesofindia.indiatimes.com/city/bengaluru/cybercrooks-dupe-79-year-old-bengaluru-woman-of-rs-35-lakh-in-ai-trading-scam/articleshow/122097772.cms (last visited on Dec. 23, 2025).

[7]Ministry of Home Affairs, "State Cyber Crime Cell Capacity Assessment Report" (2024).

[8]"Bharatiya Laws Against Deepfake Cybercrime: Opportunities and Challenges", Vivekananda International Foundation, Apr. 28, 2025, available at: https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges (last visited on Dec. 22, 2025).

[9]"Deepfake Technology in India: Navigating Legal, Ethical, and Societal Implications", PoliLegal, Jan. 24, 2025, available at: https://polilegal.com/post/deepfake-technology-in-india-navigating-legal-ethical-and-societal-implications/ (last visited on Dec. 21, 2025).

[10]"Deepfakes in India: Legal Landscape, Judicial Responses, and a Practical Playbook for Enforcement", National e-Governance Division, Sept. 29, 2025, available at: https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/ (last visited on Dec. 21, 2025).

individuals to discredit genuine evidence by claiming it is fabricated.[11] Such manipulation not only distorts voter perception but also undermines trust in democratic institutions.

IV. THE LEGAL PATCHWORK: WHAT LAWS APPLY TODAY?

A. Statutory Provisions

India doesn't have a single law that says "deepfakes are illegal." Instead, victims must rely on a fragmented set of provisions spread across multiple laws. Under the Information Technology Act, 2000,[12] Section 66D addresses cheating by impersonation using computer resources, while Section 66E deals with violations of privacy involving unauthorised capture or transmission of private images. Section 67A penalises the publication of sexually explicit content online.The Bharatiya Nyaya Sanhita, 2023,[13] offers limited recourse through general provisions on forgery, organised cybercrime, and the dissemination of false or synthetic information.

The Digital Personal Data Protection Act, 2023[14] further imposes penalties for misuse of biometric and personal data, with fines reaching up to ₹250 crore for serious violations. However, these provisions were drafted without deepfake technology in mind. They address the consequences of harm but fail to recognise the unique mechanisms and scale of AI-generated abuse.[15]

B. Judicial Responses and the Evolution of Personality Rights

In the absence of clear legislation, Indian courts have increasingly stepped in to address deepfake-related disputes. In *Ankur Warikoo v. John Doe*, the Delhi High Court granted interim relief, recognizing that deepfakes threaten both privacy and financial security.[16] Meta was directed to take down content within 36 hours and disclose user details.

In *Global Health Limited & Anr v. John Doe*, the court protected Dr. Naresh Trehan from misleading deepfakes circulating on WhatsApp.[17] The ruling expanded personality-rights

[11]M. Hameleers, et al., "You Won't Believe What They Just Said! The Effects of Political Deepfakes Embedded as Vox Populi on Social Media" 8 Social Media + Society 1 (2022).
[12]The Information Technology Act, 2000 (Act 21 of 2000).
[13]The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
[14]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[15]Shinu Vig, "Regulating Deepfakes: An Indian Perspective" 17 Journal of Strategic Security 70 (2024).
[16]*Supra* note 2.
[17]*Supra* note 3.

protection into the healthcare sector. Earlier precedents such as *Shivaji Rao Gaikwad v. Varsha Productions* helped lay the foundation for personality-rights jurisprudence in India.[18]

In *Nirmaan Malhotra v. Tushita Kaul*, the court acknowledged the 'era of deepfakes' and shifted the burden of proof regarding digital evidence.[19]

However, such remedies remain largely accessible to individuals with financial resources, entrenching inequality in access to digital justice.

V. THE OCTOBER 2025 AMENDMENTS TO THE IT RULES

In October 2025, the Ministry of Electronics and Information Technology introduced amendments to IT Rules defining "synthetically generated information" for the first time.[20] The new framework mandates that AI-generated videos must carry 10% screen watermarks saying "AI-Generated," platforms must remove reported deepfakes within 36 hours, AI tools must embed traceable metadata, and platforms must verify user claims about content authenticity. Political parties must remove deepfake posts within three hours during the Model Code of Conduct period, as per Election Commission of India directives.[21]

The Supreme Court heard a Public Interest Litigation on deepfake regulations but closed it after the Centre showcased these draft rules.[22] Critics warn that the current IT Rules are overly broad and risk flagging satire and legitimate creative content, raising concerns of censorship beyond the limits set in *Shreya Singhal case* in 2015.[23]

The core challenge is balancing harm prevention with constitutional limits on state power. The *Shreya Singhal case* emphasises that intermediary liability must be narrowly tailored and subject to judicial oversight to remain constitutionally valid.

VI. THE GENDERED COST OF DEEPFAKE ABUSE

---

[18]"Personality Rights in the Digital Age: Balancing Identity, Expression, and Control", Legal Service India, available at: https://www.legalserviceindia.com/Legal-Articles/personality-rights-in-the-digital-age-balancing-identity-expression-and-control/(last visited on Dec. 23, 2025).
[19]*Supra*note 9.
[20]"AI, Deepfake Legal Response", Law Asia, 2025, available at: https://law.asia/ai-deepfake-legal-response/ (last visited on Dec. 22, 2025).
[21]*Supra* note 11.
[22]Harmanjeet Singh and Ritu Panta, "Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent and Admissibility in Law" 7(6) International Journal for Multidisciplinary Research (2025).
[23]Shreya Singhal v. Union of India (2015) 5 SCC 1.

In India's socially conservative society, the consequences are catastrophic. The Sulli Deals and Bulli Bai cases, where images of female journalists and activists were "auctioned" for virtual sexual exploitation, exemplify the gendered weaponization of deepfake technology.[24] Journalist Rana Ayyub's cloned identity was used for targeted harassment aimed at silencing her reporting.

When a deepfaked image circulates, women face not just reputational harm but real physical risk. In honour-based and socially conservative communities, the circulation of fabricated intimate imagery can trigger consequences ranging from social ostracism to physical violence, compounding already high rates of gender-based harm.[25] The societal stigma attached to sexual violence, even when fabricated, often discourages victims from seeking whatever limited legal recourse exists.

Parliamentary committees have stressed the need for intersectional protections, noting that Dalit, Muslim and tribal women face heightened vulnerability.[26] Deepfakes mirror offline caste and communal hierarchies, demanding sensitive legal responses.

VII. COMPARATIVE PERSPECTIVES AND GLOBAL APPROACHES

Kaminski notes a core divide in AI governance, the EU's rights-based model versus the US's market-driven, sectoral approach. The EU AI Act, which came into force in 2024, classifies deepfakes as "high-risk" AI systems subject to stringent transparency and accountability requirements. The Act requires clear labelling of AI-generated content and mandates safeguards against unlawful use.

India appears to be moving toward a hybrid model combining EU-style comprehensive regulation and US-style intermediary liability. However, this hybrid model risks creating regulatory complexity without corresponding enforcement capacity. The proposed Digital India Act (still under consultation as of Dec 2025) aims to replace the IT Act and address AI content more directly.[27] Preliminary drafts indicate provisions on malicious deepfakes, digital identity protection, and platform liability.

---

[24]"Illusions of Identity: Legislative Challenges Revolving around Deepfake Technology", LawctopusAcademike, Aug. 6, 2025, available at: https://www.lawctopus.com/academike/illusions-of-identity-legislative-challenges-revolving-around-deepfake-technology/ (last visited on Dec. 23, 2025).
[25]National Crime Records Bureau, *"Crime in India 2022"* (2023).
[26]*Supra* note 11.
[27]*Supra* note 21.

China has implemented among the world's strictest deepfake regulations, requiring deepfake creators to obtain consent from subjects and mandating that all synthetic media be clearly marked.[28] However, this model carries risks of state overreach incompatible with India's constitutional guarantees.

VIII. TOWARDS A COMPREHENSIVE LEGAL FRAMEWORK

A. Legislative Imperatives

India needs a specific criminal offence targeting malicious deepfake creation, with intent clearly defined. It must differentiate harmful deepfakes from satire, parody, and artistic expression, ensuring Article 19(1)(a) protections.

Fast-track compensation mechanisms are essential to avoid years-long litigation. A dedicated digital crimes victim compensation fund, modelled on existing victim compensation schemes under the Bharatiya Nagarik Suraksha Sanhita, could provide immediate relief while criminal investigations proceed. Investment in AI detection tools and nationwide training is crucial.

Cross-border cooperation and mutual legal assistance treaties are essential due to the transnational nature of deepfakes. Public awareness campaigns must educate citizens about deepfakes and encourage critical consumption of digital media, particularly given that most people cannot identify sophisticated deepfakes without technical tools.

A technology-specific offence should incorporate the following elements:

i) a clear statutory definition of "deepfake" grounded in synthetic manipulation of biometric identity;
ii) an intent requirement distinguishing malicious creation from artistic or satirical use;
iii) a consent-based liability framework centred on unauthorised use of likeness;
iv) aggravated categories for sexual exploitation, electoral interference, and financial fraud;
v) mandatory platform traceability and metadata retention duties; and explicit extraterritorial jurisdiction provisions for cross-border enforcement.

B. Forensic and Evidentiary Reforms

[28]"Deepfake Technology in India and World: Foreboding and Forbidding", Asian Institute of Research (2025), available at: https://www.asianinstituteofresearch.org/lhqrarchives/deepfake-technology-in-india-and-world:-foreboding-and-forbidding (last visited on Jan. 8, 2026).

Law enforcement agencies lack standardized methodologies for detecting deepfakes, resulting in variable evidence quality and significant legal challenges.[29] State-level cyber cells show low technical capacity, worsening prosecution challenges. Poor conviction rates stem from evidentiary complexity, procedural delays, and limited technical expertise among investigators.

The Bharatiya Sakshya Adhiniyam, which replaced the Evidence Act on July 1, 2024, must be interpreted to account for AI-generated evidence.[30]Courts need clear standards for authenticating AI-generated evidence, including forensic review and chain-of-custody rules. Judicial capacity building is essential; few judges have the necessary technical background to analyse complex AI-related evidence without substantial expert guidance.

IX. DOCTRINAL ANALYSIS

A. The Consent Lacuna: Beyond Obscenity to Digital Dignity

India's existing legal frameworkand the realities of deepfake abuse is perhaps most starkly visible in the treatment of nonconsensual intimate imagery. Section 67A of the Information Technology Act penalises the publication of 'material containing sexually explicit act or conduct' in electronic form.[31] The wrong in nonconsensual deepfake imagery is not primarily that it is obscene; it is that a person's likeness and identity have been weaponised without their consent. By prosecuting such conduct under an obscenity framework, the law inadvertently treats the victim's dignity as a secondary concern, subordinating her autonomy to an assessment of whether community standards of decency have been offended, the test derived from the Supreme Court's formulation in Ranjit Udeshi.[32] This obscenity-centric framing has doctrinal consequences, such as deepfaked imagery that is sexual but not technically 'obscene' under that standard may escape prosecution entirely.This doctrinal gap reveals that the law's concern lies with public morality rather than individual autonomy. The Digital Personal Data Protection Act, 2023 imposes obligations concerning the processing of personal data,[33] but does not specifically address the use of a person's biometric identity to generate synthetic media. The concept of digital consent, understood as consent to the use of one's likeness, voice, and biometric data in

[29]*Supra* note 8.
[30]The BharatiyaSakshya Adhiniyam, 2023 (Act 47 of 2023).
[31]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 66.
[32]*Supra* note 4.
[33]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025, Ministry of Electronics and Information Technology, October 2025.

AI-generated content, thus remains almost entirely undeveloped in Indian jurisprudence.Comparatively, the United Kingdom's Online Safety Act 2023 and the Criminal Justice Bill 2024 have moved explicitly toward a consent-centred model, criminalising the creation and sharing of intimate synthetic images without the subject's consent.[34] India's law reform process must similarly anchor liability in the violation of consent rather than in the obscene character of the output, recognising that a woman's dignity is harmed the moment her likeness is used without authorisation, irrespective of whether the resulting content is judicially characterised as obscene.

B. Platform Liability and the Limits of Safe Harbour

Section 79 of the Information Technology Act grants intermediaries conditional immunity from liability for third-party content, provided they observe 'due diligence' and comply with takedown directions.[35] This safe harbour, modelled substantially on the American approach under the Digital Millennium Copyright Act, was designed for an environment in which platforms were passive conduits. Deepfake technology has fundamentally altered this environment, since modern social media platforms deploy algorithmic amplification systems that actively promote high-engagement content, and deepfake videos, especially those involving recognisable public figures or sexual material, frequently meet the criteria such algorithms prioritise.The platform is therefore not merely a neutral conduit; it is, in a meaningful sense, a distributor. Where algorithmic amplification is deliberate and profit-driven, continued reliance on a passive intermediary model becomes conceptually strained.The 2021 IT Rules and the October 2025 amendments mandating 36-hour takedowns[36] represent legislative acknowledgement of this shift, yet they remain reactive, as platforms act only upon notification rather than proactively deploying detection mechanisms. The EU AI Act's requirements of technical documentation and cooperation with competent authorities for general-purpose AI systems[37] provide a more proactive model. Furthermore, the 'whack-a-mole' problem by which removed content reappears across other platforms before effective removal, points toward the need for cross-platform

[34]*Supra* note 15.
[35]State of Maharashtra v. Ranjit D. Udeshi AIR 1965 SC 881.
[36]Online Safety Act 2023 (UK), s. 188; Criminal Justice Bill 2024 (UK), cl. 187.
[37]The Information Technology Act, 2000 (Act 21 of 2000), s. 79; The Digital Millennium Copyright Act, 17 U.S.C. § 512 (1998).

coordination.[38] India's proposed Digital India Act should consider mandating interoperability of takedown notifications, such that a valid removal order against one platform generates obligations for others hosting substantially identical content. Hash-matching technology, already deployed voluntarily by some platforms to detect child sexual abuse material, could be statutorily mandated for judicially verified deepfake content, transforming the current reactive regime into a genuinely preventive one.

C. The Evidentiary Challenge: Authenticity in the Age of Synthetic Media

The proliferation of deepfake technology generates a secondary legal crisis: the erosion of evidentiary trust. The BharatiyaSakshya Adhiniyam, 2024 retains provisions on electronic evidence[39] but does not address the specific challenge of AI-generated or AI-manipulated content. The court in *Nirmaan Malhotra v. Tushita Kaul* acknowledged the 'era of deepfakes'and began shifting evidentiary burdens in recognition of this challenge,[40] but such judicial innovation, absent statutory support, creates inconsistency and unpredictability across proceedings. State-level cyber cells lack standardised methodologies for detecting deepfakes, resulting in variable evidence quality and significant forensic challenges for prosecution.[41]Parliament should consider amending the BharatiyaSakshyaAdhiniyam to impose a threshold burden of production on any party seeking to rely on audio-visual evidence and requiring, before that evidence is admitted for substantive purposes, a certified forensic report establishing that the material has not been synthetically generated or materially manipulated. Such a requirement would operate as a preliminary admissibility safeguard rather than a reversal of the prosecution's ultimate burden of proof, thereby remaining consistent with constitutional criminal procedure norms.This would not displace the overall burden of proof but would create an authentication gateway proportionate to the evidentiary risks posed by deepfake technology, standardise forensic practice across jurisdictions, and reduce the scope for deepfake evidence to

[38]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(1)(b); as amended October 2025.
[39]EU AI Act (n 5), Arts. 13, 53.
[40]M. Hameleers et al., 'You Won't Believe What They Just Said! The Effects of Political Deepfakes Embedded as Vox Populi on Social Media' 8 Social Media + Society (2022).
[41]The BharatiyaSakshya Adhiniyam, 2024 (Act 47 of 2023), ss. 57–63.

distort criminal proceedings, including through the 'liar's dividend' by which genuine evidence may be dismissed as fabricated.[42]

D. Definitional Ambiguity

The absence of a clear legal framework for deepfakes creates several structural gaps. First and foremost, there is no legal definition of "deepfake" in criminal statutes. Enforcement depends heavily on officers' technological capacity and complainants' resources.[43] This definitional ambiguity leads to inconsistent enforcement.

E. Reactive Rather Than Preventive

Existing laws act only after harm occurs. There's no specific criminal liability for merely creating a deepfake with malicious intent. This creates a framework where harm is punished only after it occurs, with no deterrence against the creation of deepfakes themselves.

F. Jurisdictional Complexity

Deepfake tools and servers are frequently located outside India. When the creator is in one country, the server in another, and the victim in India then which law applies? The jurisdictional maze means most perpetrators simply walk free. Territorial jurisdiction principles do not translate well to digital offences. India's lack of comprehensive mutual legal assistance treaties with many jurisdictions further complicates cross-border enforcement.[44]

X. CONCLUSION

The deepfake crisis constitutes a fundamental stress test of India's legal system's capacity to evolve at the pace of technological change. Courts have demonstrated commendable adaptability, building on the personality rights jurisprudence laid down in *Shivaji Rao Gaikwad v. Varsha Productions*, and illustrating the judiciary's willingness to deploy existing doctrine creatively in the face of legislative silence.Yet the boundaries of judicial innovation are inherent and well-understood, courts can interpret and adapt, but they cannot create criminal offences, establish

---

[42]Nirmaan Malhotra v. Tushita Kaul, CS(COMM) 112/2024 (Delhi High Court).

[43] "Exploring Legal and Technical Challenges of Deepfake in India", International Journal for Research in Applied Science & Engineering Technology (2025), available at: https://www.ijraset.com/research-paper/exploring-legal-and-technical-challenges-of-deepfake-in-india (last visited on Jan. 8, 2026).

[44]*Supra* note 6 at 24-26.

enforcement institutions, or negotiate mutual legal assistance treaties. These are legislative and executive imperatives.

The current legal patchwork dispersed across the Information Technology Act, the Bharatiya Nyaya Sanhita, the Digital Personal Data Protection Act, and the October 2025 IT Rules, fails on multiple dimensions. It is reactive rather than preventive, addressing harm only after it has materialised and spread. It is obscenity-centric rather than consent-centred, misidentifying the core wrong in deepfake abuse. It is jurisdictionally inadequate, leaving most cross-border perpetrators beyond effective reach. And it is forensically unsupported, relying on enforcement agencies that the 2024 Capacity Assessment Report documents as lacking adequate technical capacity. The October 2025 Rules are a meaningful step, but their overbroad definitions risk sweeping satire, parody, and political commentary within their ambit, in tension with the constitutional safeguards affirmed in Shreya Singhal. The Bombay High Court's striking down of the Fact Check Unit Rule confirms that content moderation laws must be narrowly tailored and subject to independent judicial oversight.

Looking comparatively, India's legislative drafters inherit a rich body of international experience. The EU AI Act's risk-based classification and transparency obligations, the United Kingdom's consent-centred intimate image abuse provisions, and China's mandatory consent and watermarking requirements together offer useful, if partial, models. India's constitutional context, and in particular its robust free speech jurisprudence, counsels against the most restrictive elements of the Chinese approach while permitting careful adaptation of the EU's accountability architecture. India appears to be evolving toward a hybrid model, and the proposed Digital India Act must ensure that this hybrid does not produce regulatory complexity without corresponding enforcement capacity.

India requires anticipatory, consent-based, technology-specific criminal legislation, not merely to regulate emerging technology, but to safeguard constitutional dignity in the digital age.Courts have responded with creativity, but judicial innovation cannot substitute for coherent statutory design. The longer Parliament delays, the more the costs of regulatory inaction are borne by those whose digital identities remain legally unprotected.