

DEEPFAKES, PRIVACY, AND THE LAW: A CRITICAL AND COMPARATIVE ANALYSIS OF INDIA'S REGULATORY RESPONSE TO SYNTHETIC MEDIA

- Inchara S Bajal¹ & Ashwin²

ABSTRACT

The rapid diffusion of generative artificial intelligence has made the creation of hyper realistic synthetic audio, image, and video termed “deepfakes” cheap, fast, and widely accessible. What began as an area application of machine learning has, within a few years, become a significant instrument of financial fraud, political disinformation, and nonconsensual sexual imagery.

This paper synthesises and critically examines recent legal scholarship on deepfakes and privacy law in India, drawing upon publications from the International Journal of Law, Management & Humanities, the Law Times Journal, Record of Law, and broader academic literature on deepfake governance available through Research gate. It identifies areas of convergence, recurring criticisms, and emerging proposals for legal reform. The analysis suggests that India’s current regulatory response remains fragmented and largely reactive, with significant reliance on intermediary based takedown mechanisms. Existing statutes and regulatory frameworks were not specifically designed to address synthetic media, resulting in important doctrinal, regulatory, and remedial gaps in addressing deepfake related harms to privacy, reputation, and individual autonomy.

The paper comparatively examines the European Union’s General Data Protection regulation (GDPR), Digital Services Act (DSA), and, particularly, Article 50 of the Artificial Intelligence Act (AI ACT). It argues that India may benefit from a more codified, preventive, transparent, and victim centred regulatory framework. The study also identifies areas of divergence within the literature, including the role of copyright and intellectual property law, the adequacy of personality-rights jurisprudence, and the

¹ Student at St. Aloysius (Deemed To Be University), School Of Law, Mangaluru

² Assistant Professor at St. Aloysius (Deemed To Be University), School Of Law, Mangaluru

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

question of whether India should enact a dedicated deepfake statute or instead incrementally amend existing legislation.

The paper concludes with legislative, institutional, judicial, platform-level, and public-facing recommendations aimed at moving India from a largely reactive approach toward a more preventive, rights based, and effective framework for the governance of synthetic media.

1. INTRODUCTION

The contemporary digital environment increasingly challenges the traditional assumption that visual and auditory evidence can always be accepted at face value. A video may depict a public official apparently making a statement that was never made; an audio recording may convincingly imitate a bank official; and an individual's face may be digitally superimposed onto content in which the individual never participated. These developments illustrate the distinctive legal risks posed by deepfake technology, particularly in relation to privacy, reputation, identity, and the authenticity of digital evidence.

Deepfakes are synthetic media, including images, audio, and video, that are generated or manipulated using artificial intelligence and machine-learning techniques to make a person appear to say or do something that they did not actually say or do. Such techniques may include generative adversarial networks (GANs), diffusion models, and other generative AI methods³. Technological developments have substantially reduced the cost, technical expertise, and time required to create such material, enabling ordinary users to produce increasingly convincing synthetic content through widely available applications and online tools.

For India, the implications are particularly significant. The country has a large internet and social-media user base, a substantial film and celebrity economy, and growing exposure to AI-enabled voice and video fraud. At present, India does not have a dedicated, comprehensive statute specifically regulating deepfakes. Instead, the legal response is distributed across constitutional privacy jurisprudence, the Information Technology Act, 2000, the Information Technology (Intermediary

³ Annpurna & Ashok Kumar, Protecting Privacy from Deepfake Technology in India: A Critical Analysis of the Indian Legal Framework with Lessons from the European Union, 9(IV) Int'l J.L. Mgmt. & Humanities 1950 (2026); Deepfakes, AI and the Law: Protecting Privacy and Reputation in India's Evolving Legal Framework, Law Times Journal (July 31, 2026).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, the Copyright Act, 1957, and developing personality-rights jurisprudence. These existing legal frameworks may provide remedies for particular harms caused by deepfakes, but they were not specifically designed to address the full range of risks associated with synthetic media⁴.

The present study undertakes a comparative synthesis of recent contributions to the legal literature. By which two questions organize the analysis.

- First, what are the principal areas of agreement across the literature regarding the nature of deepfake-related harms, the applicable legal framework, and the direction of legal reform?
- Second, what are the principal criticisms of the existing Indian legal framework, and in which areas do the sources diverge?

This doctrinal component considers the constitutional right to privacy recognised in Justice K.S. Puttaswamy (Retd.) v. Union of India; relevant provisions of the Information Technology Act, 2000, including Sections 66C, 66D, 66E, 67, 67A, and 67B. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, including the 2025 Amendment addressing synthetically generated information; the Digital Personal Data Protection Act, 2023; the Bharatiya Nyaya Sanhita, 2023; and, where relevant, the Copyright Act, 1957. The comparative component examines the European Union's GDPR, Digital Services Act, and Artificial Intelligence Act, alongside the United Kingdom's Online Safety Act, 2023 and selected United States right-of-publicity authorities.

THE NATURE OF THE HARM: A POINT OF NEAR-CONSENSUS

The literature examined in this study demonstrates widespread recognition regarding the principal forms of privacy harm generated by deepfake technology, though scholarly treatment remains fragmented across disciplinary lines and lacks a unified taxonomy.

THREE REGISTERS OF HARM

⁴ Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India); Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended (India); Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India); Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India); Copyright Act, No. 14 of 1957, Acts of Parliament, 1957 (India).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

Drawing on the three facets of privacy recognised in Puttaswamy case⁵, Physical, informational, and decisional, this paper identifies three principal registers of deepfake harm:

- (1) informational privacy, through unauthorised extraction and synthetic recombination of biometric data;
- (2) bodily privacy and dignity, through non-consensual sexual imagery; and
- (3) reputational harm, through fabricated attribution of statements or conduct.

The IJLMH paper identifies three principal registers of deepfake harm: informational privacy, decisional and bodily privacy, and reputational or associational privacy. The Record of Law article similarly draws on Puttaswamy case to frame deepfake harms across informational privacy, decisional autonomy, and dignitary privacy.

The wider information further supports the significance of non-consensual intimate imagery and biometric identity compromise. These examples demonstrate how a technological act of synthetic manipulation can produce lasting consequences for privacy, dignity, reputation, and personal security⁶.

The Disproportionate Impact On Women

An area of convergence concerns the gendered character of deepfake harm. The literature repeatedly identifies women as disproportionately affected by nonconsensual intimate imagery (NCII) and synthetic sexual deepfakes. Such material may cause severe dignitary, psychological, professional, and social consequences, while also being capable of rapid and repeated online dissemination. Peer-reviewed literature⁷ on deepfake pornography treats non-consensual synthetic sexual imagery as one of the most urgent areas requiring legislative intervention. Scholarship in this area argues that existing privacy and data protection laws are insufficient and advocates criminalisation as a distinct offence.

THE “LIAR’S DIVIDEND” AND THE EROSION OF EVIDENTIARY TRUST

One concern is the phenomenon commonly described as the “liar’s dividend.” The existence of convincing deepfake technology enables a person to dismiss genuine audio-visual evidence as fabricated, while allowing fabricated content to be presented as

⁵ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

⁶ Information Technology Act, 2000, Sec. 66C, 66D, 66E, 67, 67A, 67B

⁷Dr. Rituparna Bhattacharjee & Ms. Muskan Sharma, Deepfake & Pornography: The Coming Crisis of Privacy and Consent, South Eastern European Journal of Public Health 1196–1213 (2025), <https://doi.org/10.70135/seejph.vi.4885>.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

authentic. The problem therefore extends beyond individual privacy and affects criminal investigations, judicial proceedings, journalism, and democratic discourse⁸.

The appropriate legal response is not to assume that all digital evidence is unreliable. Rather, the increasing sophistication of synthetic media reinforces the need for reliable forensic authentication, provenance mechanisms, metadata analysis, hash verification, and competent expert evidence — while recognising that such measures authenticate the integrity of the record, not necessarily the truth of the event depicted.

THE RASHMIKA MANDANNA INCIDENT

Several sources identify the November 2023 incident involving the digital superimposition of actress Rashmika Mandanna's face onto a video originally featuring British-Indian influencer Zara Patel as a significant catalyst for public and regulatory attention in India. The incident illustrated the speed with which synthetic content can circulate and the vulnerability of individuals whose likenesses are misappropriated without consent⁹.

Beyond the shared diagnosis of harm, the literature converges on a common set of regulatory objectives, consent, platform accountability though it diverges sharply on the doctrinal mechanisms through which those objectives transparency should be pursued. The EU adopts a regulatory-administrative model, the US a property-tort model, and India currently relies on judicial personality rights doctrine supplemented by delegated legislation.

CONSTITUTIONAL FOUNDATION: PUTTASWAMY AS COMMON GROUND

The Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, constitutes the principal constitutional foundation for privacy claims involving synthetic media. The judgment predates the emergence of deepfakes as a mass phenomenon, and its application to synthetic media therefore requires significant doctrinal extension to address harms inflicted by private actors, violations of bodily integrity and dignity, and remedies for synthetic impersonation, dimensions the judgment did not directly contemplate.

Subramanian Swamy v. Union of India, (2016) 7 SCC 221, is relevant to the protection of reputation as an aspect of Article 21, and thus to the dignitary and

⁸ Supra1

⁹ Supra 5

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

reputational harms deepfakes inflict¹⁰. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, is equally important because any deepfake-specific restriction affecting expression must satisfy the rigorous standard articulated therein, proximate relationship to an Article 19(2) ground and no impermissible chilling effect on protected speech.

4.2 THE INFORMATION TECHNOLOGY ACT AS A STRUCTURAL MISFIT

The Information Technology Act, 2000 provides several potentially relevant provisions, including Section 66C on identity theft, Section 66D on cheating by personation using a computer resource, Section 66E on violation of privacy, and Sections 67, 67A, and 67B concerning prohibited categories of electronic content. While these provisions predate the emergence of deepfakes, they remain the primary statutory basis for addressing synthetic media harms, supplemented by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and their 2026 amendments¹¹.

These provisions were drafted for technological conditions materially different from those associated with generative artificial intelligence. Section 66E is principally concerned with the "capture" or "transmission" of images, and its elements presuppose an image of a private area captured from a real person. In the deepfake context whether superimposing a real face onto another person's body, or generating sexualized imagery lacking any authentic source of capture. The "capture" element faces interpretive difficulty: in the former case, the "private area" of the person whose face is superimposed was never captured; in the latter case, there is no original material that could have been captured.

The Digital Personal Data Protection Act, 2023: Relevant But Incomplete

The Digital Personal Data Protection Act, 2023 is relevant because facial characteristics, voiceprints, and other identifying attributes may constitute personal data. Nevertheless, the Act does not comprehensively address the output-side harms caused by synthetic media.

First, data-protection law primarily regulates the processing of personal data, whereas the circulation of an already-created deepfake raises a distinct content-related problem. Secondly, statutory penalties are not designed as a direct compensation

¹⁰ A. Bhattathiri, F. Sharma & A. Purohit, *Deepfake in the Courtroom: Legal Challenges and Evidentiary Standards*, in *Digital Doppelgangers: The Rise of Deepfakes & Artificial Intelligence* (Lex Assisto Media and Publications), 10–24

¹¹ *Deepfakes, AI and the Law: Protecting Privacy and Reputation in India's Evolving Legal Framework*, *Law Times Journal* (July 31, 2026);

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

mechanism for the individual victim. Thirdly, the institutional structure of data-protection enforcement does not by itself provide a specialised mechanism for determining whether particular synthetic media is authentic, defamatory, or otherwise unlawful.

These limitations demonstrate that data-processing regulation and content-specific regulation should be understood as complementary rather than interchangeable.

THE INTERMEDIARY GUIDELINES: A “CATCH-UP” MODEL

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have become a principal practical mechanism for addressing harmful online content. Their significance lies in the ability of platforms to remove or restrict access to unlawful content upon receiving actual knowledge in the form of a court order or government notification, thereby providing a practical remedy where the creator is anonymous or difficult to identify. The extremely compressed timelines introduced by the 2026 amendments have raised concerns that platforms may overremove content to preserve safe harbour protection, implicating the free speech safeguards articulated in *Shreya Singhal Case*¹².

Content may already have been created, uploaded, copied, and widely circulated before a complaint is processed. The effectiveness of the framework may also vary according to platform size, technical capacity, jurisdiction, and the speed of grievance handling. Recent regulatory developments concerning synthetically generated information and platform labelling represent movement toward greater transparency. These mechanisms remain substantially post-creation and post-upload in character.

JUDICIAL CREATIVITY THROUGH PERSONALITY RIGHTS

Indian courts, particularly the Delhi and Bombay High Courts, have developed significant personality-rights jurisprudence relevant to synthetic media. Authorities including *Anil Kapoor v. Simply Life India*, *Aishwarya Rai Bachchan v. Aishwaryaworld.com*, *Jaikishan, Kakubhai Saraf alias Jackie Shroff v. The Peppy Store*, and *Arijit Singh v. Codible Ventures LLP* demonstrate judicial willingness to protect names, images, voices, and other elements of personal identity. Notably, this protection has not been confined to celebrities. The Delhi High Court has confirmed that the doctrine extends to any identifiable individual whose identity possesses commercial or personal value.

¹² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Such cases frequently involve urgent injunctions, including John Doe or Ashok Kumar orders, against unknown or future infringers. In the absence of a comprehensive statutory framework, this jurisprudence represents a form of judicial adaptation — courts applying constitutional and common-law principles to novel technological harms through flexible procedural mechanisms rather than awaiting legislative intervention.

At the same time, access to such remedies may be uneven. Celebrities and persons possessing substantial commercial recognition may be better positioned to establish personality-rights claims and obtain urgent judicial relief than ordinary individuals. This creates an access-to-justice concern, particularly because non-celebrity individuals are frequent targets of non-consensual intimate deepfakes, with empirical studies indicating that the vast majority of deepfake abuse victims are not public figures.

Principal Comparative Benchmark

The European Union is repeatedly identified as the principal comparative benchmark. The GDPR, Digital Services Act, and Artificial Intelligence Act together demonstrate a more codified approach to data protection, platform responsibility, transparency, and synthetic-content disclosure, though the literature also identifies significant enforcement gaps and implementation asymmetries within this framework.

The comparative lesson is not that Indian law should mechanically reproduce the European framework. Rather, the EU model illustrates the value of clear statutory definitions, preventive transparency obligations, direct civil remedies, and institutional accountability. The UK Online Safety Act and United States right-of-publicity jurisprudence provide additional comparative perspectives.

SIMILAR CRITICISMS:

THE CONSOLIDATED CASE AGAINST THE STATUS QUO

The literature reveals several recurring criticisms of India's current approach to deepfakes. A principal deficiency is the absence of a comprehensive definition of "deepfake" or "synthetically generated content" in primary legislation. While the 2026 IT Amendment Rules introduce the first statutory definition of "synthetically generated information," this definition operates only through delegated legislation binding intermediaries, leaving the person whose likeness has been taken without a directly enforceable remedy. A clear definition in primary legislation would establish the scope of regulatory obligations and reduce uncertainty regarding the distinction between lawful synthetic expression and unlawful manipulation.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Where fundamental rights are affected, primary legislation also provides greater democratic legitimacy and stability than reliance exclusively upon subordinate rules or executive advisories.

5.2 REACTIVE, TAKE-DOWN-CENTRED DESIGN

The second recurring criticism is the reactive character of the existing framework. Platform-level removal generally occurs after content has been created and disseminated, which may be inadequate where harmful material spreads rapidly across multiple platforms and accounts. While the 2026 IT Amendment Rules introduce proactive elements mandatory labelling, metadata embedding, and pre-publication verification of SGI declarations, the takedown mechanism itself remains reactive in its trigger, requiring a court order or government intimation before removal obligations arise.

The literature therefore favours a preventive model that incorporates transparency and disclosure obligations at the stage of creation or deployment, while retaining effective post-publication takedown procedures. Indian law does not presently provide a single, specialised, fast, and victim-oriented compensation mechanism for deepfake harms comparable to the civil compensation framework associated with Article 82 of the GDPR. Injunctions may provide immediate protection, but ordinary victims may face significant procedural, financial, and evidentiary barriers. A coherent framework should therefore consider both removal and monetary redress.

Fragmented And Uncoordinated Institutional Responsibility

Responsibility for deepfake-related harms is dispersed among multiple institutions, including the Ministry of Electronics and Information Technology, data-protection authorities, police cybercrime units, and constitutional courts. The absence of a single coordinating institutional mechanism may produce delays, duplication, and uncertainty regarding responsibility. A specialised or coordinating authority could improve technical capacity, investigation, standards, and inter-agency cooperation.

ABSENCE OF A WORKABLE TYPOLOGY

A further concern is the lack of a clear statutory distinction between malicious, transformative, and benign synthetic media. While the 2026 IT Amendment Rules introduce exclusions for routine editing, educational and research content, and accessibility improvements, the extremely compressed three-hour takedown timeline may still incentivise platforms to remove first and review later¹³. This creates a chilling

¹³ Annpurna & Ashok Kumar, *supra* note 1; Deepfakes, AI and the Law, Law Times Journal. For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

effect that could unintentionally burden legitimate artistic, journalistic, educational, research, satirical, or cinematic uses, even where the content falls outside the express exclusions.

A future framework should therefore adopt a proportionate and technology-neutral classification based on purpose, consent, harm, and risk.

5.6 INTELLECTUAL PROPERTY AS AN ADJACENT AREA OF CONCERN

The literature diverges regarding the weight that copyright and intellectual-property law should receive. Some sources focus principally on privacy and personality rights, while others address authorship, AI training datasets, copyright infringement, and moral rights¹⁴.

This divergence is better understood as a difference in scope rather than a contradiction. Deepfake regulation implicates a bundle of legal interests, including privacy, dignity, reputation, personality, intellectual property, and evidentiary integrity. Nevertheless, in a privacy-focused analysis, intellectual property remains an adjacent rather than the central doctrinal issue.

RECOMMENDATIONS AND REGULATORY SAFEGUARDS

The following recommendations are directed to the principal stakeholders implicated in deepfake governance.

- For Legislators And Regulators
 - A statutory, primary-legislation definition of “deepfake” or “synthetically generated content” should be enacted rather than leaving the principal definition exclusively to delegated rule-making. Disclosure and labelling obligations should attach, where appropriate, to the creation or deployment of synthetic media and should complement existing platform-level takedown duties.
 - A direct civil compensation mechanism should be considered for victims of unlawful non-consensual synthetic media. Such a mechanism should recognise that state-imposed regulatory penalties and victim compensation serve different purposes.

Facial geometry, voiceprints, gait, and comparable biometric attributes should receive heightened protection in contexts involving AI training and generation, subject to

¹⁴ AI-Generated Deepfakes in India: Consent, Privacy, and the Limits of Existing Cyber Regulation, Int'l J.L. Mgmt. & Humanities (2026).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

a clear statutory framework and meaningful consent requirements. At present, however, the DPDP Act, 2023 contains no sensitive-data tier, and the Act does not specifically define or distinguish biometric data from other forms of personal data. The 2026 IT Amendment Rules address synthetically generated information but do not impose heightened obligations regarding biometric inputs to AI training. The absence of a statutory sensitive data category means that facial geometry, voiceprints, and gait patterns currently receive no greater protection than ordinary personal data.

Regulatory responsibility should be coordinated through a technically competent institutional mechanism capable of receiving complaints, directing investigations, coordinating with platforms and law-enforcement agencies, and imposing appropriate sanctions. The NAITRA Bill, 2024 proposes precisely such a body, vesting it with civil court-like powers and a mandate to prohibit high-risk AI applications including deepfakes. At present, however, no such coordinating mechanism exists in Indian law, and responsibility remains dispersed among MeitY's advisory committee, the Data Protection Board, and Grievance Appellate Committees.

A statutory typology should distinguish malicious synthetic media, transformative expression, and benign applications. Obligations should be proportionate to the level of risk and the rights affected. A fast-track, low-cost grievance mechanism should be developed for non-consensual intimate synthetic media so that urgent protection is not practically available only through High Court litigation¹⁵.

Digital forensic verification should be strengthened through recognised procedures involving hash verification, metadata analysis, provenance checks, chain-of-custody safeguards, and qualified expert testimony. Legislation should avoid placing the principal regulatory burden upon executive advisories or delegated rule-making where mandatory obligations, financial penalties, or significant restrictions upon lawful expression require a stable statutory foundation.

Any deepfake-specific legislation should be narrowly and carefully drafted so that it does not inadvertently criminalise legitimate artistic, journalistic, satirical, educational, research, or cinematic expression. Constitutional standards concerning freedom of speech and expression must remain central to the legislative design¹⁶. Data-processing regulation

¹⁵ Morbiwala & Vidya Sagvekar, Exploring Legal and Technical Challenges of Deepfake in India, 13 Int'l J. for Rsch. in Applied Sci. & Eng'g Tech. 124 (2026)

¹⁶ Dr. Rituparna Bhattacharjee & Ms. Muskan Sharma, Deepfake & Pornography: The Coming Crisis of Privacy and Consent, South Eastern European Journal of Public Health 1196–1213 (2025)

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

should not be treated as a complete substitute for contentspecific regulation. Consent and purpose limitations address the processing of personal data, but do not by themselves provide a complete remedy after harmful synthetic media has entered public circulation.

Platform safe-harbour withdrawal should not be the sole enforcement mechanism. A dedicated or coordinated authority with investigative and sanctioning capacity is necessary to address anonymous creators, cross-border platforms, and repeated dissemination.

Finally, remedies should be designed around the ordinary victim rather than primarily around persons possessing pre-existing commercial reputations. The legitimacy of a deepfake framework depends upon its accessibility to persons without the financial capacity to commence urgent constitutional litigation.

- COURTS

Courts should continue developing personality-rights and John Doe/Ashok Kumar injunction jurisprudence while encouraging consistent procedural practices for urgent synthetic-media cases. Relief should recognise that informational, dignitary, bodily, and reputational harms may coexist in a single incident. Judicial approaches to disputed digital evidence should increasingly rely upon forensic verification rather than unaided visual or auditory assessment¹⁷. Metadata, hashes, provenance information, expert evidence, and chain-of-custody material should be considered where appropriate.

Existing statutory provisions may, where doctrinally defensible, be interpreted purposively pending legislative clarification. However, such interpretation should remain consistent with statutory language and constitutional limitations.

The absence of a dedicated deepfake statute should not automatically result in judicial inaction where existing constitutional, statutory, or common-law principles provide a lawful basis for relief. At the same time, emergency ex parte remedies should be designed with awareness of access-to-justice concerns¹⁸. The “liar’s dividend” should not justify a presumption that all digital evidence is unreliable. Rigorous authentication is preferable to a blanket rejection of electronic evidence.

- PLATFORMS AND INTERMEDIARIES

Platforms should establish proactive detection systems for high-risk categories, including non-consensual intimate imagery, election-related synthetic content, and

¹⁷ Supra 13

¹⁸ Ibid

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

financial-fraud deepfakes. Machine-readable metadata, provenance tracking, and visible labelling should be incorporated where technically feasible and legally required. The 2026 IT Amendment Rules have introduced mandatory detection obligations for SSIMs and mandated labelling and metadata embedding for permitted SGI. However, the "technically feasible" qualifier creates compliance uncertainty, the mandatory detection obligation may amount to prior restraint, and the rules bind intermediaries alone without creating directly enforceable rights for victims¹⁹.

Notice-and-takedown systems should be accessible, clearly publicised, and responsive. Platforms should provide realistic timelines, effective escalation mechanisms, and appropriate appellate routes. Platform obligations should be proportionate to size, reach, and technical capacity. Larger and more resource-intensive platforms may reasonably be subject to enhanced duties concerning detection, compliance personnel, provenance, and transparency. Platforms should cooperate with lawful law-enforcement and judicial requests, including where content is hosted across jurisdictions.

User self-declaration that content is synthetic should not be treated as a sufficient verification mechanism where independent safeguards are reasonably available. Complaints should not disappear into opaque or inaccessible internal processes, particularly where the creator is unidentified or the platform is foreign-based. Compliance requirements should avoid a uniform, one-size-fits-all approach that either imposes disproportionate burdens on small platforms or permits major platforms to operate below appropriate standards. A graduated regulatory model is therefore preferable.

- INDIVIDUAL USERS AND THE PUBLIC

Individuals should independently verify suspicious audio or video content, particularly urgent requests for money, one-time passwords, or sensitive information. Verification should occur through an independent communication channel rather than through the same potentially compromised medium.

Victims should promptly report non-consensual synthetic content through applicable platform grievance mechanisms and, where appropriate, to law-enforcement

¹⁹ Comparative framework: GDPR, Digital Services Act, Artificial Intelligence Act, Online Safety Act 2023 (UK), and selected United States right-of-publicity authorities including *Midler v. Ford Motor Co.*, 849 F.2d 460

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

or cybercrime authorities²⁰. Evidence such as screenshots, URLs, timestamps, and copies of relevant communications should be preserved where lawful and safe to do so.

Users should remain conscious of the digital footprint created by publicly available photographs and recordings, recognising that such material may be collected or misused. This awareness, however, should never be interpreted as shifting responsibility from the perpetrator to the victim. Public digital-literacy initiatives should be supported to improve the ability of individuals to recognise, question, and appropriately report suspected synthetic media.

Individuals should not assume authenticity merely because audio-visual content appears convincing. They should also avoid forwarding suspected non-consensual or defamatory synthetic content, even for the purpose of “debunking,” because further circulation may compound the underlying harm. The absence of a dedicated deepfake statute does not necessarily mean that no legal remedy exists. Constitutional privacy principles, personality rights, and relevant statutory provisions may provide possible avenues of relief depending upon the facts.

TOWARD A COHERENT INDIAN FRAMEWORK CONSOLIDATED RECOMMENDATIONS

A synthesis of the reform proposals examined in this paper yields five principal recommendations.

- First, Parliament should consider enacting a statutory definition of synthetic and AI-manipulated media within the Information Technology Act or a dedicated AI statute. Primary legislation would provide greater legal certainty and a stronger foundation for obligations concerning transparency, labelling, and liability.
- Secondly, a mandatory and technology-neutral labelling obligation, informed by the transparency approach of Article 50 of the EU AI Act, should apply at the point of dissemination and should supplement existing platform-level detection and takedown duties.
- Thirdly, the Digital Personal Data Protection Act, 2023 should be complemented by clear protections for biometric attributes used in AI

²⁰ As stated in Digital Personal Data Protection Act, 2023; Information Technology Act, 2000; Bharatiya Sakshya Adhinyam, 2023

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

training and generation, together with an accessible mechanism for victim compensation where unlawful processing or related misuse causes legally recognised harm.

- Fourthly, a fast-track and low-cost grievance mechanism should be established for non-consensual intimate synthetic media. Such a mechanism should enable ordinary victims to obtain urgent assistance without being functionally dependent upon immediate High Court litigation. While the 2026 IT Amendment Rules mandate two-hour takedown for NCII and the MeitY SOP provides victim-centric reporting pathways, these mechanisms remain dispersed across platform grievance officers, One Stop Centres, the NCRP, and law-enforcement channels. No single specialised body currently coordinates urgent relief for NCII victims. A dedicated fast-track mechanism would consolidate these pathways and ensure that ordinary victims can obtain urgent protection without recourse to High Court litigation.
- Fifthly, institutional responsibility should be coordinated through an appropriate authority or expanded mandate capable of bringing together data protection, platform regulation, technical investigation, and law-enforcement functions. India has explicitly chosen a "convergence" model, distributing responsibility across I4C, the Data Protection Board, GACs, the SAHYOG portal, and state police, rather than establishing a single coordinating authority. The Data Protection Board, while formally constituted, is not yet functional, and its mandate is confined to data protection without powers over platform regulation or technical investigation. The NCW has recommended a comprehensive restructuring, but this remains a proposal. Your recommendation would require a deliberate departure from India's current institutional design.

The objective should not be to prohibit synthetic media as a category. Rather, the regulatory objective should be to distinguish legitimate technological and expressive uses from conduct that unlawfully violates privacy, dignity, reputation, autonomy, or other protected interests.

Conclusion

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

The literature examined in this paper presents a remarkably consistent assessment of India's current response to deepfakes. Indian courts, particularly the Delhi and Bombay High Courts, have demonstrated significant doctrinal creativity in applying constitutional privacy principles and personality-rights jurisprudence to emerging forms of synthetic-media harm.

Judicial innovation, however, cannot substitute indefinitely for a coherent legislative and regulatory architecture. This is particularly important for ordinary, non-celebrity victims who may lack both the resources and the commercial basis necessary to obtain rapid personality-rights relief. The absence of a specialised, accessible, compensatory remedy remains a significant concern.

The European model demonstrates the potential value of combining primary-legislation definitions, ex ante transparency obligations, direct civil remedies, and coordinated regulatory enforcement. Nevertheless, the European framework cannot simply be transplanted into India without accounting for differences in institutional capacity, federal structure, platform diversity, and the scale of India's digital population.

The principal lesson is therefore functional rather than transplant-based: privacy protection against deepfakes is likely to be more effective when regulation operates at the stages of creation, deployment, and disclosure, rather than only after a complaint has been made. India's evolving framework provides an opportunity to move toward a preventive, rights-based approach, provided that reform is anchored in clear legislation, supported by meaningful compensation, and designed around the ordinary victim as well as public figures.

Reference:

1. Annpurna & Ashok Kumar, Protecting Privacy from Deepfake Technology in India: A Critical Analysis of the Indian Legal Framework with Lessons from the European Union, 9(IV) Int'l J. L. Mgmt. & Humanities 1950 (2026).
2. Roshan Gupta, Deepfakes, AI and the Law: Protecting Privacy and Reputation in India's Evolving Legal Framework, Law Times Journal (Aug. 1, 2026).
3. Aditya Rathi, The Legal Implications of Deepfakes: Protecting Privacy and Intellectual Property in the Age of Generative AI, Record of Law (June 3, 2026).
4. Deepfake & Pornography: The Coming Crisis of Privacy and Consent, ResearchGate (2024).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

5. Sheikh Inam Ul Mansoor, Legal Implications of Deepfake Technology: In the Context of Manipulation, Privacy, and Identity Theft, ResearchGate (2024).
6. The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology, ResearchGate (2025).



For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>