Page 1950 - 1964

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Protecting Privacy from Deepfake Technology in India: A Critical Analysis of the Indian Legal Framework with Lessons from the European Union

ANNPURNA* AND PROF. DR. ASHOK KUMAR**

ABSTRACT

The growth of generative artificial intelligence has made the fabrication of hyper-realistic synthetic audio, image and video content, commonly termed "deepfakes", cheap, fast and widely accessible. The non-consensual synthetic appropriation of a person's face, voice and image has created a distinct category of privacy harm, endangering informational privacy, bodily autonomy, reputation and, disproportionately, women's dignity. Although India is one of the largest markets for digital content and among the nations most affected by deepfake-enabled fraud and non-consensual imagery, it continues to rely on a disjointed and largely reactive legal framework constructed from the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 as amended, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, and judge-made personality-rights jurisprudence. This paper undertakes a doctrinal and comparative analysis of that framework against the more codified regime of the European Union, comprising the General Data Protection Regulation, the Digital Services Act and, most significantly, Article 50 of the Artificial Intelligence Act, which imposes direct, ex ante transparency and labelling obligations on deepfake deployers. Drawing on recent Delhi and Bombay High Court rulings that recognise personality rights as a component of the right to privacy, as well as on empirical data concerning the extent of deepfake-related fraud and abuse in India, the paper argues that the Indian framework is deficient in definitional clarity, in preventive rather than reactive design, and in victim-centred remedies. The proposals derived from the European experience include a statutory definition and labelling requirement for synthetic material, codified platform accountability outside safe-harbour litigation, and a specific civil remedy for non-consensual synthetic media.

Keywords: *Deepfakes, Privacy, Digital Personal Data Protection Act 2023, Information Technology Rules, European Union AI Act, GDPR, Synthetic Media.*

* Author is a Research Scholar at Central University of South Bihar, Gaya, Bihar, India.
** Author is a Professor at Central University of South Bihar, Gaya, Bihar, India.

 [ISSN 2581-5369]

I. INTRODUCTION

Deepfakes are synthetic media generated or manipulated using machine-learning techniques, most commonly generative adversarial networks, in a manner that causes a person to appear to say or do something they never said or did. What began as a specialised academic and entertainment tool has, within a few years, become a common instrument of financial fraud, political deception and, most unsettling of all, non-consensual sexual imagery. A believable face-swap or voice clone can now be produced from a handful of photographs or a few seconds of audio using freely available applications.[1]

For India, the stakes are unusually high. The country has one of the world's largest bases of internet and social-media users,[2] a vibrant film and celebrity economy whose personas are readily scraped for training data, and a citizenry that has already shown itself acutely vulnerable to AI-enabled voice and video fraud. Yet India has no standalone deepfake statute. Its response has instead been assembled, piecemeal, from data protection law, intermediary regulation, criminal law and an evolving body of High Court precedent on personality rights.[3] The European Union, by contrast, has moved towards a codified, *ex ante* model: the Artificial Intelligence Act, Regulation (EU) 2024/1689, contains a direct, horizontally applicable transparency obligation for deepfakes under Article 50,[4] layered atop the consent and purpose-limitation architecture of the General Data Protection Regulation and the platform-accountability regime of the Digital Services Act.

This paper pursues two connected questions. First, is the existing Indian legal architecture doctrinally adequate to protect individual privacy against deepfake-enabled harm? Second, what can India's ongoing regulatory reform, including the amendments to the Intermediary Guidelines carried through by the Ministry of Electronics and Information Technology in 2025 and 2026,[5] usefully borrow from the more mature, rights-based model of the European Union?

The argument developed here is that although Indian courts have shown considerable doctrinal creativity in extending privacy and personality rights to synthetic media, the legislative and executive response remains reactive, take-down-centric and insufficiently victim-oriented, and

[1] Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1758-60, 1768-86 (2019).
[2] DATAREPORTAL, *Digital 2025: India* (Feb. 25, 2025), https://datareportal.com/reports/digital-2025-india.
[3] Chesney & Citron, *supra* note 1, at 1786-1819.
[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) art. 50, OJ L, 2024/1689, 12.7.2024.
[5] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India) (in force Feb. 20, 2026).

 [ISSN 2581-5369]

that the European transparency-by-design model offers lessons that are instructive without being directly transplantable.

II. Research Methodology

This study combines doctrinal, comparative and empirical (case-study and statistical) research.

The doctrinal component examines the principal legal sources governing privacy and synthetic media in India: constitutional provisions, statutes, delegated legislation and judicial decisions. The materials examined include the Information Technology Act, 2000, in particular Sections 66C, 66D, 66E, 67 and 67A,[6] the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 together with their subsequent amendments,[7] the Digital Personal Data Protection Act, 2023,[8] and the relevant provisions of the Bharatiya Nyaya Sanhita, 2023.[9]

The comparative component benchmarks the Indian framework against the General Data Protection Regulation,[10] the Digital Services Act[11] and the Artificial Intelligence Act[12] of the European Union, with particular attention to the deepfake-transparency obligations in Article 50 of the Artificial Intelligence Act, which became applicable on 2 August 2026, and to the accompanying Code of Practice on Transparency of AI-generated Content.[13] The comparison is functional rather than mechanical: it asks how each jurisdiction allocates the burden of disclosure, consent and remedy among creators, deployers and platforms.

The empirical component draws on secondary quantitative data from industry and civil-society surveys on the prevalence of deepfake fraud and abuse in India, and on a series of case studies from recent Delhi and Bombay High Court litigation, in order to show how the doctrinal framework functions, and fails to function, in practice.

---

[6] The Information Technology Act, No. 21 of 2000, §§ 66C, 66D, 66E, 67, 67A (India).

[7] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India), as amended by G.S.R. 275(E) (Apr. 6, 2023), G.S.R. 775(E) (Oct. 22, 2025) and G.S.R. 120(E) (Feb. 10, 2026).

[8] The Digital Personal Data Protection Act, No. 22 of 2023 (India).

[9] The Bharatiya Nyaya Sanhita, No. 45 of 2023 (India).

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[11] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

[12] Artificial Intelligence Act, *supra* note 4, arts. 3(60), 50, 113 (Chapter IV applying from Aug. 2, 2026).

[13] European Commission, *Code of Practice on Transparency of AI-generated Content* (June 10, 2026); see also European Commission, *Opinion on the Assessment of the Code of Practice on Transparency of AI-generated Content* (July 9, 2026).

 [ISSN 2581-5369]

III. Deepfake Technology and the Nature of the Privacy Harm

Deepfake harm to privacy operates on at least three distinct registers.[14]

The first is informational privacy in the conventional data-protection sense: a person's face, voice and biometric pattern are personal, often sensitive, data, and their extraction and synthetic recombination without consent is a form of unauthorised processing.

The second is decisional and bodily privacy: non-consensual sexually explicit deepfakes appropriate a person's likeness in a manner that violates dignity and autonomy irrespective of whether any data breach in the technical sense has occurred.

The third is reputational and associational privacy: deepfakes can falsely attribute statements, endorsements or conduct to a person, causing harm that resembles defamation but is procedurally and evidentially more difficult to contest because the underlying content looks authentic.

It is rare for these three registers to operate separately. A single viral deepfake, such as an altered video purporting to show a public figure making a statement, can serve as a vehicle for financial fraud or disinformation while simultaneously constituting an attack on dignity, an unlawful processing of biometric data and a reputational injury. It is this layered quality that presents the central doctrinal difficulty examined in this paper: a harm arising on several registers at once is not readily controlled by any single legal instrument.

IV. The Indian Legal Framework

A. Constitutional Foundation

The doctrinal starting point for any privacy claim in India is the nine-judge bench decision of the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[15] which held the right to privacy to be intrinsic to the right to life and personal liberty under Article 21 of the Constitution,[16] encompassing informational privacy, bodily autonomy and decisional autonomy. Although *Puttaswamy* did not address synthetic media, its articulation of privacy as protecting an individual's control over their own identity and self-presentation supplies the constitutional predicate on which lower courts have since relied, directly or indirectly, when granting relief against the deepfake misuse of a person's image and voice.

[14] Mengqi Han, *The Infringement of Deepfake Technology on Personal Privacy and Legal Protection: A Discussion Based on Article 1032 of the Civil Code*, 41 J. Educ., Human. & Soc. Sci. 188, 188-97 (2024).
[15] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[16] India Const. art. 21.

 [ISSN 2581-5369]

B. The Information Technology Act, 2000

The Information Technology Act remains the principal statute addressing cyber-harms, but it was drafted well before deepfake technology existed and contains no reference to synthetic or AI-generated content. Section 66E[17] penalises capturing, publishing or transmitting the image of a person's private area without consent, but its language centres on capturing an actual image rather than synthetically generating one, which creates an interpretive gap for wholly fabricated content. Sections 66C and 66D,[18] dealing with identity theft and cheating by personation using a computer resource, have been more readily extended to deepfake-enabled fraud, since impersonation through synthetic voice or video fits comfortably within their language. Sections 67 and 67A,[19] penalising the publication of obscene and sexually explicit material in electronic form, have similarly been invoked against non-consensual sexual deepfakes, though again without any express statutory acknowledgment that the underlying image may be synthetic rather than real.

C. Intermediary Guidelines and the 2023 to 2026 Amendments

Because identifying and prosecuting an anonymous deepfake creator is often practically impossible, the principal lever of Indian regulation has become intermediary liability under Section 79 of the Information Technology Act, operationalised through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[20] Platforms that fail to act on flagged synthetic content within the prescribed timelines risk losing the safe-harbour protection that otherwise shields them from liability for user content. In December 2023 the Ministry of Electronics and Information Technology issued a formal advisory reminding intermediaries of their due-diligence obligations under Rule 3(1)(b) in relation to misinformation and deepfakes, though that advisory carried no independent statutory force.[21]

A more structural intervention began with the draft amendments released for public consultation in October 2025, which introduced, for the first time, a definition of "synthetically generated information": information artificially or algorithmically created, generated, modified or altered using a computer resource in a manner that makes it reasonably appear to be authentic or true.[22]

---

[17] The Information Technology Act, *supra* note 6, § 66E.
[18] *Id.* §§ 66C, 66D.
[19] *Id.* §§ 67, 67A.
[20] The Information Technology Act, *supra* note 6, § 79; Intermediary Guidelines, *supra* note 7, rr. 3(1)(b), 3(1)(d).
[21] MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, *Advisory to Intermediaries and Platforms on Due Diligence Obligations in Relation to Misinformation and Deepfakes* (Dec. 26, 2023) (India).
[22] MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, *Explanatory Note: Proposed Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in Relation to Synthetically Generated Information* (Oct. 22, 2025) (India) (proposed r. 2(1)(wa)).

 [ISSN 2581-5369]

Those amendments were notified on 10 February 2026 and came into force on 20 February 2026. They provide that references to information in Rules 3(1)(b), 3(1)(d), 4(2) and 4(4) include synthetically generated information; they require an intermediary offering a computer resource that enables the creation of such information to ensure that it carries a prominent and readily perceivable visual label, or, for audio content, a prefixed audio disclosure, together with embedded permanent metadata bearing a unique identifier; and they place a further duty on significant social media intermediaries to obtain a user declaration as to whether uploaded content is synthetically generated, to deploy reasonable technical measures to verify that declaration, and to label content so confirmed.[23] The quantitative labelling test canvassed in the October 2025 draft, under which a visible label was to occupy at least a tenth of the display surface or the opening tenth of an audio track, did not survive into the notified rules. Industry bodies have objected that the amendments convert what were previously advisory instruments into binding obligations without direct parliamentary enactment, an objection that echoes a live constitutional debate about the limits of delegated rule-making under the Information Technology Act.

Even with these reforms, the Indian approach remains structurally reactive. It obliges platforms to detect and label content after creation and upload, rather than regulating the tools of creation themselves or vesting individuals with a freestanding statutory right against the non-consensual synthetic replication of their likeness.

D. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, India's first comprehensive data protection statute, does not mention deepfakes, but a person's facial geometry, voice pattern and other biometric attributes fall within its broad definition of personal data.[24] On this reading, an entity that scrapes a person's photographs or voice recordings in order to train or run a deepfake-generation model is processing personal data and qualifies as a data fiduciary subject to the Act's obligations of purpose limitation, data minimisation, notice and consent. Data principals enjoy rights of correction and erasure, and the Act permits the nomination of another individual to exercise the rights of a deceased or incapacitated person, which is relevant given how frequently deepfakes are generated using images of deceased public figures.[25]

The enforcement architecture of the Act nonetheless has significant limits for deepfake victims. Monetary penalties under the Schedule, which rise to Rs 250 crore for the most serious breaches,

[23] Amendment Rules, 2026, *supra* note 5, rr. 2(1A), 3(3), 4(1A).
[24] The Digital Personal Data Protection Act, *supra* note 8, § 2(t).
[25] *Id.* §§ 12, 14.

 [ISSN 2581-5369]

are credited to the Consolidated Fund of India rather than paid to the victim,[26] so the statute provides no direct compensatory remedy comparable to a tort claim or to the right to compensation conferred by Article 82 of the General Data Protection Regulation.[27] The jurisdiction of the Data Protection Board is likewise concerned with regulating the processing conduct of fiduciaries rather than with adjudicating the authenticity or defamatory character of specific synthetic media, which means that victims must still pursue parallel civil or criminal remedies to obtain a takedown or an injunction. The Act was not designed with deepfakes in mind, and applying it to synthetic media therefore requires a degree of interpretive extension that leaves meaningful gaps, particularly around biometric-specific safeguards, the oversight of AI training datasets, and the question whether purely synthetic, as opposed to scraped, biometric likeness is covered at all.

E. The Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023, which came into force on 1 July 2024,[28] replaced the Indian Penal Code, 1860,[29] and retains, and in places sharpens, provisions relevant to deepfakes. The defamation provisions apply where a morphed image or video damages reputation, regardless of whether the underlying content is AI-generated. The provisions on cheating by personation and on forgery extend to digitally fabricated identity documents, images or communications used to deceive. The provisions addressing insults to the modesty of a woman and voyeurism, carried forward with amendments from the erstwhile Penal Code, have been invoked in cases involving morphed intimate images, although their language continues to centre on the capturing of an image rather than on its synthetic creation, a textual gap that continues to generate interpretive difficulty for prosecutors.

F. Personality Rights as Privacy Protection

In the absence of a dedicated statute, the High Courts, principally at Delhi and Bombay, have developed a substantial body of personality-rights jurisprudence that constitutes the most concrete judicial response to deepfakes. In *Anil Kapoor v. Simply Life India*,[30] the Delhi High Court granted an *ex parte* injunction restraining the unauthorised commercial use of the actor's name, image, voice and catchphrase, and expressly extended protection to AI-generated deepfakes, ringtones and GIFs, holding that an individual has an inherent and enforceable right

[26] *Id.* §§ 33(1), 34 & sch. entry 1.
[27] General Data Protection Regulation, *supra* note 10, art. 82.
[28] The Bharatiya Nyaya Sanhita, *supra* note 9, §§ 77, 79, 319, 336, 356; S.O. 850(E) (Feb. 23, 2024) (India) (bringing the Sanhita into force on July 1, 2024).
[29] The Indian Penal Code, No. 45 of 1860 (India), repealed by The Bharatiya Nyaya Sanhita, *supra* note 9, § 358(1).
[30] *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914 (India).

 [ISSN 2581-5369]

to control the commercial exploitation of his own personality. The Court reasoned that personality rights are both a moral and an economic asset, so that the parasitic commercial appropriation of a person's identity through generative tools cannot be tolerated.

That reasoning was carried further in *Aishwarya Rai Bachchan v. Aishwaryaworld.com*,[31] in which the Delhi High Court granted an *ex parte* interim injunction against websites, e-commerce sellers and a chatbot that impersonated the actress, including through sexually explicit AI-generated conversations. The Court held that the claimant had established a strong *prima facie* case, that the unauthorised exploitation of her personality caused both financial loss and a violation of dignity and privacy, and that a failure to grant urgent interim relief would cause irreparable harm. Comparable interim protection has since been extended by the Delhi High Court to a number of other public figures, as in *Jaikishan Kakubhai Saraf alias Jackie Shroff v. The Peppy Store*,[32] and by the Bombay High Court to performers including the playback singer in *Arijit Singh v. Codible Ventures LLP*,[33] whose voice had been cloned by generative tools. Such relief is typically granted through "John Doe", or "Ashok Kumar", orders that bind unnamed and future infringers as well as named defendants.

A widely discussed illustration of the everyday dimension of the problem is the viral video circulated in November 2023 in which the face of the actress Rashmika Mandanna was digitally superimposed on another woman's body, a video so convincing that its synthetic origin was not obvious to ordinary viewers. The episode, though it too involved a public figure, demonstrated how readily the same technique could be deployed against a private individual with no comparable capacity to secure urgent judicial relief. It underscores that the personality-rights doctrine, built around commercially valuable celebrity personas, offers less certain footing for ordinary citizens whose claim rests on dignity and privacy alone rather than on economic goodwill.

Taken together, this case law demonstrates two things. First, the Indian courts have shown genuine doctrinal agility, assembling protection from performers' rights under the Copyright Act, the Trade Marks Act, the constitutional right to privacy and ordinary tort principles, without waiting for legislative intervention. Second, that protection remains structurally uneven. It is fastest and most robust for individuals with the resources to litigate and the celebrity status on which an economic personality-rights claim can be founded, and comparatively thin for ordinary citizens, disproportionately women, who are the most frequent targets of non-

[31] *Aishwarya Rai Bachchan v. Aishwaryaworld.com*, 2025 SCC OnLine Del 5943 (India).
[32] *Jaikishan Kakubhai Saraf alias Jackie Shroff v. The Peppy Store*, 2024 SCC OnLine Del 3664 (India).
[33] *Arijit Singh v. Codible Ventures LLP*, 2024 SCC OnLine Bom 2445 (India).

 [ISSN 2581-5369]

consensual sexual deepfakes but the least likely to secure a rapid *ex parte* injunction from a High Court.

V. The European Union Framework

A. The General Data Protection Regulation

The General Data Protection Regulation supplies the foundational layer of European deepfake regulation. Biometric data processed for the purpose of uniquely identifying a natural person is classified as a special category of personal data under Article 9, attracting heightened protection and, ordinarily, a requirement of explicit consent for processing.[34] The principles of purpose limitation and data minimisation in Article 5 constrain the scraping of images and voice samples for the training of generative models,[35] while the right to erasure in Article 17[36] and the right to object in Article 21[37] give data subjects the means to demand the removal of their biometric likeness from training or generation pipelines. Critically, Article 82 confers a direct right to compensation for material or non-material damage arising from an infringement,[38] a private civil remedy that has no close equivalent in the Digital Personal Data Protection Act, 2023.[39]

B. Article 50 of the Artificial Intelligence Act

The centrepiece of the European Union's deepfake-specific regulation is Article 50 of the Artificial Intelligence Act, whose transparency obligations became applicable across the member states on 2 August 2026.[40] Article 50(4) requires deployers of an AI system that generates or manipulates image, audio or video content constituting a deepfake to disclose that the content has been artificially generated or manipulated.[41] The Act defines a deepfake, in Article 3(60), as AI-generated or manipulated image, audio or video content resembling existing persons, objects, places, entities or events that would falsely appear to a person to be authentic or truthful.[42] Where the content forms part of an evidently artistic, creative, satirical or fictional work, the disclosure obligation is calibrated rather than waived: the deployer must still disclose the existence of the generated or manipulated content, but may do so in a manner that does not hamper the display or enjoyment of the work.

---

[34] General Data Protection Regulation, *supra* note 10, art. 9(1), (2)(a).
[35] *Id.* art. 5(1)(b)-(c).
[36] *Id.* art. 17.
[37] *Id.* art. 21.
[38] *Id.* art. 82(1).
[39] The Digital Personal Data Protection Act, *supra* note 8.
[40] Artificial Intelligence Act, *supra* note 4, arts. 50, 113.
[41] *Id.* art. 50(4).
[42] *Id.* art. 3(60).

 [ISSN 2581-5369]

Non-compliance carries substantial financial exposure. Infringement of the transparency obligations attracts administrative fines of up to EUR 15 000 000 or, where the offender is an undertaking, up to three per cent of total worldwide annual turnover for the preceding financial year, whichever is higher,[43] and the obligation reaches providers and deployers established outside the Union where the output produced by the system is used within it.[44] The implementation guidelines issued by the European Commission clarify that the labelling duty applies irrespective of any intention to deceive: content that looks or sounds like a real person must be labelled once it meets the statutory definition, whatever the deployer's motive.[45] A voluntary Code of Practice on Transparency of AI-generated Content, developed through a multi-stakeholder process facilitated by the AI Office and assessed by the Commission and the AI Board in July 2026 as adequately covering the relevant obligations, offers signatories a recognised, though not conclusive, route to demonstrating compliance, covering both visible labelling and machine-readable marking for detection purposes.[46]

What distinguishes Article 50 doctrinally from the Indian approach is its allocation of the disclosure duty directly to the deployer of the AI system, that is, to the person or entity that puts the deepfake into circulation, rather than routing enforcement solely through platform intermediary liability. This creates a horizontal, *ex ante* obligation that attaches at the point of content generation and dissemination, independent of whether a complaint is ever filed or a court order ever sought.

C. The Digital Services Act

The Digital Services Act complements the Artificial Intelligence Act by imposing systemic risk-assessment and mitigation obligations on very large online platforms and search engines,[47] requiring them to assess and address risks including the dissemination of illegal content and manipulated media capable of affecting civic discourse or public security, and by requiring hosting services generally to provide accessible notice-and-action mechanisms for affected individuals.[48] Unlike the more informal, complaint-driven takedown model under the Indian Intermediary Guidelines, the obligations of the Digital Services Act are backed by a dedicated supervisor, the European Commission in the case of very large platforms, with direct

[43] *Id.* art. 99(4)(g).
[44] *Id.* art. 2(1)(c).
[45] EUROPEAN COMMISSION, *Guidelines on Transparency Obligations for Providers and Deployers of AI Systems* (July 20, 2026), following EUROPEAN COMMISSION, *Draft Guidelines on the Implementation of the Transparency Obligations for Certain AI Systems Under Article 50 of the AI Act* (May 8, 2026).
[46] Code of Practice, *supra* note 13.
[47] Digital Services Act, *supra* note 11, arts. 34, 35.
[48] *Id.* arts. 16, 56(2), 74.

 [ISSN 2581-5369]

investigatory and sanctioning powers, rather than relying primarily on the threat of withdrawn safe-harbour protection as the enforcement mechanism.

D. Comparative Synthesis

Three structural differences emerge from this comparison.

First, the European Union regulates the deepfake itself, through a horizontally applicable definition and a labelling duty, whereas India regulates deepfakes only indirectly, through the general categories of unlawful content or personal data under instruments that were not drafted with synthetic media in mind, with a statutory definition of synthetic content emerging only now, and through delegated rule-making rather than primary legislation.[49]

Second, the European Union gives individuals a direct and monetisable civil remedy through Article 82 of the General Data Protection Regulation, while Indian data protection penalties flow to the State rather than to the victim, leaving injunctive relief under judge-made personality rights as the primary and resource-intensive avenue for individual redress.[50]

Third, European enforcement is centralised in dedicated regulators, namely the data protection authorities, the AI Office and the Commission under the Digital Services Act, each with power to impose turnover-linked fines, whereas Indian enforcement remains dispersed across the Data Protection Board, the rule-making and advisory powers of the Ministry of Electronics and Information Technology, police cybercrime units, and an increasingly burdened High Court docket of personality-rights litigation.

Table 1 summarises this comparison across five regulatory features.

Regulatory feature	India	European Union
Statutory definition of "deepfake" or synthetic content	Only through the delegated amendments to the Intermediary Guidelines of 2025 and 2026; not in primary legislation	Codified in Article 3(60) of the AI Act (primary legislation)
Ex ante labelling duty on deployers	Emerging, through the labelling obligations placed on significant social media intermediaries under the 2026 amendments; largely post-upload	Yes. Article 50(4) of the AI Act, enforceable from 2 August 2026, attaches at the point of deployment
Direct victim compensation for data misuse	No direct statutory right; penalties under the Digital Personal Data Protection Act are payable to the State	Yes. Article 82 of the GDPR gives data subjects a right to compensation
Dedicated centralised regulator	Fragmented across the Ministry of	Yes. The AI Office and

[49] Amendment Rules, 2026, *supra* note 5, r. 3(3).
[50] General Data Protection Regulation, *supra* note 10, art. 82; The Digital Personal Data Protection Act, *supra* note 8, § 34.

Regulatory feature	India	European Union
with turnover-linked fines	Electronics and Information Technology, the Data Protection Board and police cybercrime units	Commission under the AI Act, data protection authorities under the GDPR and the Commission under the DSA, with fines up to 3 per cent of global turnover
Primary current remedy for individuals	Judge-made personality-rights injunctions from the High Courts	Statutory transparency duty plus GDPR erasure and compensation rights

Table 1: Comparative snapshot of the Indian and European Union regulatory approaches to deepfakes.

VI. Scale of the Problem in India

Quantitative evidence, drawn largely from industry and civil-society sources rather than from official government statistics, indicates that deepfake-enabled harm in India is both large in scale and growing rapidly. Analysis of AI-enabled scams in India found that 47 per cent of Indian adults reported having been a victim of, or personally knowing a victim of, an AI voice-cloning or deepfake scam, nearly double the reported global average of 25 per cent, and that 83 per cent of Indian victims of such voice scams suffered a monetary loss, with almost half losing more than Rs 50,000.[51] Separately, the 2026 Thales Data Threat Report found that 65 per cent of Indian organisations had already experienced a deepfake-driven incident and that 55 per cent reported reputational damage from AI-generated misinformation or impersonation campaigns.[52]

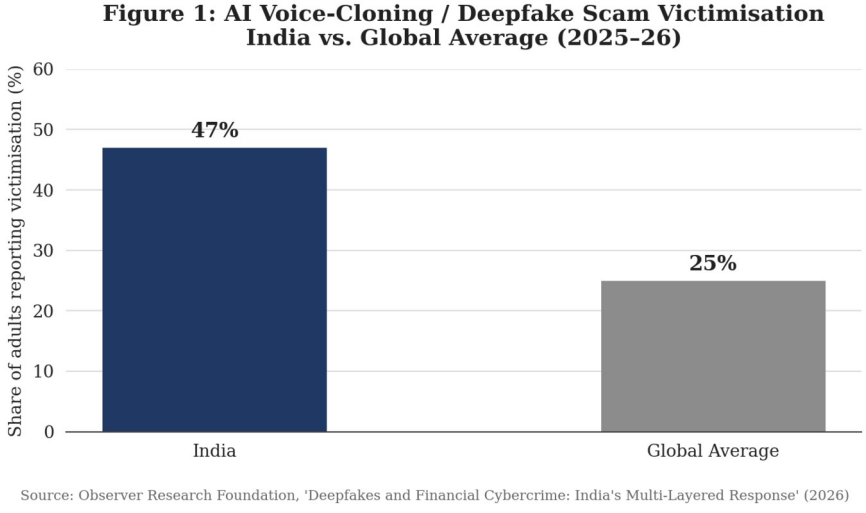

Figure 1: AI voice-cloning and deepfake scam victimisation. India reports nearly double the global average.

[51] Pranoy Jainendran, *Deepfakes and Financial Cybercrime: India's Multi-Layered Response*, Observer Research Foundation (Jan. 15, 2026), https://www.orfonline.org/english/expert-speak/deepfakes-and-financial-cybercrime-india-s-multi-layered-response. The underlying survey figures originate in McAfee, *Beware the Artificial Imposter* (2023).

[52] Thales Group, *2026 Thales Data Threat Report* (Mar. 2026) (India findings; research conducted by S&P Global Market Intelligence).

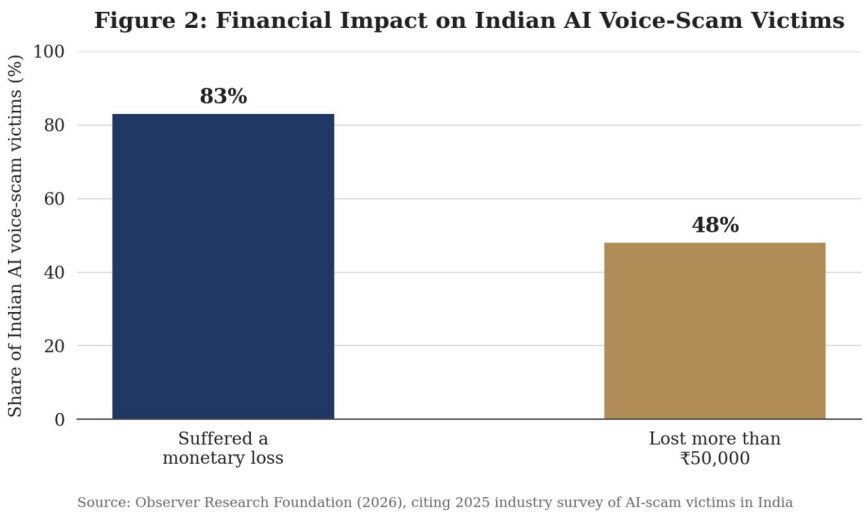

Figure 2: Financial impact on Indian AI voice-scam victims.

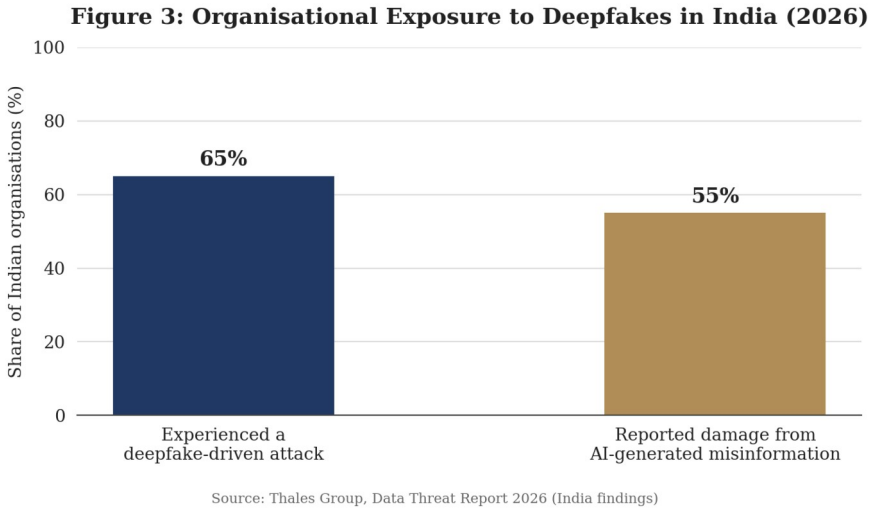

Figure 3: Organisational exposure to deepfakes in India (2026).

These figures derive from industry surveys and threat-intelligence vendors with a commercial interest in highlighting the scale of the problem; sample sizes and methodologies are not always disclosed, and cross-study comparability is limited. Nonetheless, the consistency of direction across independent sources, namely rapid year-on-year growth, a disproportionate impact relative to global averages, and a concentration in financial fraud and non-consensual imagery, supports the doctrinal argument that the existing Indian legal response has not kept pace with the scale of the harm.

VII. Gaps in the Indian Framework

Drawing the doctrinal and empirical analysis together, five structural gaps stand out.

The first is definitional absence at the level of primary legislation. "Synthetically generated information" has only recently been defined, and only through a delegated amendment to the

Intermediary Guidelines rather than by an Act of Parliament, which raises the legitimacy and stability concerns that industry bodies have already voiced.

The second is the absence of a direct, victim-payable compensatory remedy analogous to Article 82 of the General Data Protection Regulation,[53] which leaves injunctive relief under judge-made personality rights as the practical default.

The third is an intermediary-centred enforcement design that depends on content having already been created, uploaded and flagged, rather than attaching disclosure obligations at the point of generation, as Article 50 of the Artificial Intelligence Act does.[54]

The fourth is uneven access to judicial remedy. Rapid High Court relief is realistically available mainly to claimants who can mount a personality-rights claim grounded in commercial reputation, which is a poor fit for ordinary victims of non-consensual sexual deepfakes.

The fifth is the absence of a dedicated, sector-neutral regulator with turnover-linked sanctioning power comparable to the AI Office or the data protection authorities of the European Union. Enforcement responsibility is currently split across the Ministry of Electronics and Information Technology, the nascent Data Protection Board and the police, without any single body accountable for deepfake harms as such.[55]

VIII. SUGGESTIONS

Building on the European comparison while remaining attentive to India's distinct constitutional and institutional context, five recommendations follow.

First, Parliament should enact a statutory definition of synthetic and AI-manipulated media directly in the Information Technology Act or in a dedicated AI statute, rather than leaving the definition to delegated rule-making, so as to give the obligation a firmer legal foundation and reduce the risk of a successful constitutional challenge.

Second, a mandatory, technology-neutral labelling obligation modelled on Article 50 of the Artificial Intelligence Act should be placed on the deployer of a deepfake-generation tool at the point of dissemination, rather than relying solely on platform-level detection after upload.

Third, the Digital Personal Data Protection Act should be amended, or interpreted through binding guidance from the Data Protection Board, to recognise facial geometry, voiceprint and

[53] General Data Protection Regulation, *supra* note 10, art. 82.
[54] Artificial Intelligence Act, *supra* note 4, art. 50(4).
[55] Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act: Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, 22 COMPUTER L. REV. INT'L 97 (2021).

 [ISSN 2581-5369]

gait as sensitive personal data attracting heightened consent requirements specifically in the context of AI training and generation, alongside a direct compensatory remedy payable to affected data principals.

Fourth, a fast-track, low-cost grievance mechanism, potentially housed within the Grievance Appellate Committee structure created under the Intermediary Guidelines,[56] should be established specifically for non-consensual intimate synthetic media, so that non-celebrity victims are not dependent on being able to afford High Court litigation in order to obtain an urgent takedown.

Fifth, regulatory responsibility for deepfake harms should be consolidated, whether through an expanded mandate for the Data Protection Board or through a new coordinating authority, so as to avoid the current diffusion of accountability across the Ministry, the Board and state police cybercrime cells.

IX. Conclusion

Through the personality-rights doctrine, the Indian judiciary has demonstrated that existing constitutional and common-law materials can be stretched to answer at least some of the harms that deepfake technology creates. But judicial improvisation is not a substitute for a coherent legislative and regulatory architecture, particularly for the large population of ordinary, non-celebrity victims who cannot easily invoke that doctrine. The European model, comprising a defined category of synthetic content, an *ex ante* labelling duty attaching to deployers under the Artificial Intelligence Act, a direct civil remedy under the General Data Protection Regulation and centralised, turnover-linked enforcement, is not costlessly transplantable into the Indian context, given differences in institutional capacity, federal structure and the sheer scale of India's user base. Even so, its core insight is directly relevant: protection of privacy against deepfakes is most effective when it operates at the point of creation and disclosure, and not only at the point of complaint. As the amendments to the Intermediary Guidelines begin to introduce a statutory concept of synthetically generated information, India has an opportunity to move from a reactive, takedown-based model towards the kind of preventive, rights-based framework that the European Union has begun to operationalise, provided that the reform is anchored in primary legislation, accompanied by a genuine compensatory remedy, and designed with the ordinary, non-celebrity victim, and not only the litigating celebrity, in mind.

*****

[56] Intermediary Guidelines, *supra* note 7, r. 3A (inserted by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022, G.S.R. 794(E) (Oct. 28, 2022) (India)).

 [ISSN 2581-5369]