



INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 5 | 2026

Art. 09

Regulating Deepfake Advertisements: Consumer Protection and Platform Liability in India

Saleha Haneef

*Law Student, BA.LL.B., 5th Year,
Faculty of Law, Integral University, Lucknow*

Recommended Citation

Saleha Haneef, *Regulating Deepfake Advertisements: Consumer Protection and Platform Liability in India*, 5 IJHRLR 94-106 (2026).
Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto & Co. administrator.

For more information,
please contact submission.ijhrlr@gmail.com

Regulating Deepfake Advertisements: Consumer Protection and Platform Liability in India

ABSTRACT

The convergence of generative artificial intelligence and digital advertising has produced a new and largely unregulated harm: the deepfake advertisement, in which a synthetically generated voice, face, or likeness often of a recognisable public figure is used to endorse a product, service, or investment scheme without consent. Unlike earlier forms of misleading advertising, deepfake advertisements exploit consumer trust in a manner that traditional truth-in-advertising rules were never designed to address, while distributing primarily through social media intermediaries whose liability regime was built around user-generated rather than AI-synthesised commercial content. The paper examines whether India's consumer protection and intermediary liability framework principally the Consumer Protection Act, 2019, the Guidelines for Prevention of Misleading Advertisements and Endorsements, 2022, the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 adequately addresses this harm. Using a doctrinal method, this research has evaluated some of the legal provisions, rulings on the issue of personality rights, as well as the self-regulating advertising norms, juxtaposing them against EU's Artificial Intelligence Act and the FTC rule of 2024, which prohibits fake and AI-generated endorsements. Drawing on empirical data on deepfake-enabled financial fraud in India, the study finds that existing protections are fragmented, reactive, and calibrated to penalties disproportionately low relative to the scale of consumer harm, and that platform due-diligence obligations remain insufficiently tailored to paid commercial content. It recommends a statutorily defined category of "deepfake advertisement" as an unfair trade practice, turnover-linked penalties, mandatory advertiser verification for financial and health-related promotions, and coordinated enforcement among the Central Consumer Protection Authority, the Ministry of Electronics and Information Technology, and sectoral regulators.

KEYWORDS

Consumer Protection, Deepfake Advertising, Intermediary Liability, Personality Rights, Synthetic Media Regulation.

INTRODUCTION

In September 2025, a Bengaluru-based investor lost over ₹3.75 crore after encountering an online video in which a widely recognised spiritual leader appeared to endorse a trading platform; the endorsement, and the platform itself, were entirely fabricated using generative artificial intelligence.¹ The incident is not an aberration. India's Indian Cyber Crime Coordination Centre recorded cyber-fraud losses of approximately ₹22,495 crore in 2025 alone, drawn from about 2.81 million complaints,² and industry estimates suggest that deepfake-enabled financial fraud in India could approach ₹70,000 crore.³ Globally, deepfake investment-fraud schemes overwhelmingly propagated through social media advertisements impersonating celebrities, executives, and financial commentators account for the largest single category of documented deepfake losses.⁴

These figures capture a distinct and under-theorised species of consumer harm: the deepfake advertisement. Unlike a conventional misleading advertisement, which distorts facts about a product, a deepfake advertisement fabricates the very persona that lends the product credibility, an actor's face, a public figure's voice, or an entirely synthetic "virtual influencer" and does so at a cost and speed that traditional advertising fraud never permitted. Unlike non-consensual intimate imagery or election disinformation, which have received sustained regulatory and judicial attention in India, commercial deepfakes occupy an uneasy space between consumer protection law, intermediary liability law, and the common-law-derived jurisprudence of personality rights.

India's regulatory response has evolved rapidly but unevenly. The Consumer Protection Act, 2019 and the Guidelines for Prevention of Misleading Advertisements and Endorsements, 2022 govern misleading advertisements and endorser liability but were drafted without reference to synthetic media. The Information Technology (Intermediary

¹ Ken Jon Miyachi, "Trust in the Digital Age", Deccan Herald, *available at*: <https://www.deccanherald.com/amp/story/opinion%2Ftrust-in-the-digital-age-3796065> (Last visited on 5 August 2026).

² Ministry of Home Affairs and Indian Cyber Crime Coordination Centre data, cited in "India Scams 2026: Fake Cops, Deepfake Tycoons, and the ₹22,500-Crore Fraud Epidemic", *available at*: <https://scamwatchhq.com/india-scams-2026-digital-arrest-upi-fraud-epidemic/> (Last visited on 5 August 2026).

³ Pi-Labs Report, cited in Deccan Herald, "Deepfake Financial Fraud in India Could Top ₹70,000 Crore by 2025, Report Warns", *available at*: <https://www.deccanherald.com/opinion/deepfake-the-new-face-of-financial-fraud-3674748> (Last visited on 5 August 2026).

⁴ Surfshark, "AI Deepfake Losses", *available at*: <https://surfshark.com/research/chart/ai-deepfake-losses> (Last visited on 5 August 2026).

Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 introduced, for the first time, a statutory category of “synthetically generated information” together with labelling and takedown obligations,⁵ while the Advertising Standards Council of India has released draft risk-based labelling guidelines specifically for AI-generated advertising content.⁶ Meanwhile, courts principally the Delhi High Court have developed an ad hoc jurisprudence of personality rights to grant emergency injunctions against unauthorised AI-generated endorsements.⁷

This study asks whether these disparate strands amount to an adequate regulatory response, or whether deepfake advertising continues to fall through the gaps between consumer protection, platform regulation, and personality-rights litigation. It proceeds in five further parts: a review of existing scholarship, an account of methodology, a critical analysis of the statutory, judicial and comparative framework, findings, and practical recommendations for reform.

LITERATURE REVIEW

Existing academic and professional scholarships on deepfakes in India has predominantly focussed on three themes: non-consensual intimate imagery and the adequacy of Article 21-based remedies against “nudifying” websites,⁸ the misuse of synthetic media in electoral misinformation, and the judicial recognition of personality and publicity rights following *Anil Kapoor v. Simply Life India & Ors.*⁹ Commentary on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 has similarly focused on takedown timelines and safe-harbour risk for intermediaries generally, rather than on the specific interaction between synthetic-content obligations and advertising law.¹⁰

⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (10 February 2026).

⁶ Advertising Standards Council of India, Draft Guidelines for Responsible Labelling of AI-Generated Content in Advertising (2026), reported in “ASCI Releases Draft Guidelines for Responsible Labelling of AI-Generated Advertising Content”, available at: <https://www.medianews4u.com/asci-releases-draft-guidelines-for-responsible-labelling-of-ai-generated-advertising-content/> (Last visited on 5 August 2026).

⁷ See generally, “AI, Deepfakes, and Personality Rights in India: What Courts Are Doing Without a Statute”, Candour Legal, available at: <https://candourlegal.com/ai-deepfakes-personality-rights-india-courts-2026/> (Last visited on 5 August 2026).

⁸ Ritwik Sharma, “Rethinking Judicial Approaches to Sexually-Explicit Deepfakes: The Case For Article 21-Based Relief Against Nudifying Websites”, Law School Policy Review, available at: <https://lawschoolpolicyreview.com/2026/02/23/rethinking-judicial-approaches-to-sexually-explicit-deepfakes-the-case-for-article-21-based-relief-against-nudifying-websites/> (Last visited on 5 August 2026).

⁹ *Anil Kapoor v. Simply Life India & Ors.*, 2023 SCC OnLine Del 6914.

¹⁰ “Regulating Synthetic Content: Key Implications of the IT Rules Amendment, 2026”,

Industry analyses of the Advertising Standards Council of India's 2026 draft guidelines provide a detailed explanation of the proposed risk-based labelling taxonomy but, being written primarily for compliance audiences, do not situate the framework within the broader architecture of the Consumer Protection Act, 2019.¹¹ Comparative scholarship on the European Union's Artificial Intelligence Act and the Federal Trade Commission's 2024 testimonial rule exists largely in isolation from Indian consumer-law commentary, leaving open the question of what India's fragmented framework would look like when benchmarked against these more codified transparency regimes. However, the existing literature does not comprehensively examine that treats the deepfake advertisement as a discrete category of consumer harm distinguishable from non-consensual intimate imagery, electoral disinformation, and personality-rights infringement generally and evaluates it jointly through the lens of misleading-advertisement law and intermediary due diligence. Accordingly, this study addresses this gap by synthesising statutory, judicial, and self-regulatory sources into a single analytical account, and by testing that account against contemporary empirical data on deepfake-enabled commercial fraud.

RESEARCH METHODOLOGY

Research Design: This study adopts a doctrinal legal research methodology complimented by analytical research design and comparative legal analysis and secondary empirical data. It examines primary legal sources which includes legislation, subordinate rules, regulatory guidelines, and judicial decisions, alongside secondary sources including fraud-trend reports and contemporaneous professional commentary.

Sources of Data: The data is based on primary sources like the Consumer Protection Act, 2019; the Information Technology Act, 2000; the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and its 2026 Amendment; the Digital Personal Data Protection Act, 2023; misleading-advertisement guidelines by the CCPA, draft guidelines of ASCI, and certain decisions of the Delhi High Court. The secondary sources are documents produced by the Indian Cyber Crime Coordination Centre, Surfshark, Sumsb, and some recent legal and industry reviews.

Scope: This study restricts itself to commercial applications of deepfake

ANM Global, available at: <https://anmglobal.net/regulating-synthetic-content-key-implications-of-the-it-rules-amendment-2026/> (Last visited on 5 August 2026).

¹¹ "AI in Advertising: ASCI's New Draft Disclosure Guidelines", Lexology, available at: <https://www.lexology.com/library/detail.aspx?g=733f8311-c492-48bf-8a26-76f535c9247b> (Last visited on 5 August 2026).

technology in India with a comparison with the EU and the USA. It does not examine non-commercial cases of deepfakes with respect to politics, intimate images made without consent, or the parody business, apart from those required for creating jurisprudence regarding personality rights.

Limitations: The regulation of deepfakes is still evolving with rules like the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 having been introduced only in February 2026 and the ASCI guidelines being in a draft form till mid-of-2026.

Analytical Framework: The article analyses the issue through two complimentary legal lenses, i.e. consumer protection law focusing on deception and redress, and intermediary liability law focusing on platform due diligence and safe harbour protections, supplemented by a comparative transparency-regulation framework.

RESEARCH OBJECTIVES

- (i) To identify the distinct legal characteristics of deepfake advertisements as a category of consumer harm;
- (ii) To critically evaluate the adequacy of India's consumer protection, intermediary liability, and self-regulatory advertising framework in addressing this harm;
- (iii) To examine the extent to which Indian judicial developments on personality rights supplement statutory gaps;
- (iv) To compare India's approach with the European Union and the United States; and
- (v) To propose practical legal and policy reforms.

RESEARCH QUESTIONS

- (i) Does Indian law recognise the deepfake advertisement as a distinct unfair trade practice, or is it addressed only incidentally through general misleading-advertisement and intermediary-liability provisions?
- (ii) Are the penalties as well as obligations of platforms pursuant to the Consumer Protection Act, 2019 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 commensurate with the seriousness of deepfake-enabled commercial frauds in India?

- (iii) What importance has personality-rights litigation served in filling regulatory lacunae, and what are its drawbacks as a mode of consumer protection?
- (iv) What lessons does comparative regulation in the European Union and the United States offer for reform of the Indian framework?

DISCUSSION AND ANALYSIS

A. Statutory and Regulatory Architecture

India's response to deepfake advertisements is distributed across four regulatory instruments that were not designed to interact with one another. First, the Consumer Protection Act, 2019 defines a “misleading advertisement” broadly enough to capture false or deceptive endorsements,¹² and empowers the Central Consumer Protection Authority to penalise manufacturers, advertisers, and endorsers, up to ₹10 lakh for a first contravention and ₹50 lakh thereafter, with power to debar an endorser from endorsing for up to three years.¹³ The Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 extend this endorser liability to influencers and require that an endorsement reflect the endorser's genuine and current opinion based on adequate information¹⁴, is a requirement that a synthetic, AI-generated “endorser” can never, definitionally, satisfy, since it has no opinion to disclose.

Second, the Information Technology Act, 2000 governs the platforms through which deepfake advertisements circulate. Section 79 grants intermediaries safe harbour from liability for third-party content, conditional on observance of due diligence obligations prescribed under the Intermediary Guidelines.¹⁵ Until 2026, those obligations made no reference to AI-generated content; MeitY's advisory of 26 December 2023 addressed deepfakes only through the general obligation to act against “misinformation” under Rule 3(1)(b) of the 2021 Rules, without a statutory definition of the term.¹⁶ The Information Technology

¹² Consumer Protection Act, 2019, s. 2(28).

¹³ Consumer Protection Act, 2019, s. 21.

¹⁴ Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022, F. No. J-25/4/2020-CCPA (Reg) (9 June 2022), available at: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1832906®=48&lang=2> (Last visited on 5 August 2026).

¹⁵ Information Technology Act, 2000, s. 79.

¹⁶ Ministry of Electronics and Information Technology, Advisory No. 2(4)/2023-CyberLaws-2 (26 December 2023), available at: <https://www.pib.gov.in/PressReleaselframePage.aspx?PRID=1990542> (Last visited on 5 August 2026).

(Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 remedied this gap by introducing a defined category of “synthetically generated information,” mandatory visible labelling and tamper-resistant provenance metadata, and a compressed three-hour takedown window for the most harmful categories of unlawful synthetic content, with a two-hour window for non-consensual intimate deepfakes.¹⁷ Compliance with these obligations is now folded into the due-diligence conditions for retaining safe harbour under Section 79, meaning that a platform's failure to label or act on a deepfake advertisement can, in principle, expose it to liability.¹⁸

Third, the Digital Personal Data Protection Act, 2023 supplies an indirect layer of protection: because a synthetic advertisement typically depends on processing an individual's voice, image, or biometric likeness, personal data under the Act, its creation without consent may separately violate the Act's consent requirements, independent of any advertising-specific claim.¹⁹

Fourth, self-regulation through the Advertising Standards Council of India has moved fastest of all. ASCI's May 2026 draft guidelines adopt a three-tier, risk-based labelling taxonomy: high-risk uses (fabricated endorsements, unauthorised deepfakes, fake authority figures such as fictitious doctors) are prohibited outright regardless of labelling; medium-risk uses (virtual influencers, AI-cloned likeness or voice, synthetic product demonstrations) require prominent disclosure such as “Audio/Video created using AI”; and low-risk uses (routine editing, decorative effects) require no label at all.²⁰ As an industry self-regulatory code, however, ASCI's guidelines carry no statutory penalty and bind only ASCI's voluntary membership.

B. Judicial Developments: Personality Rights as a Stopgap

In the near-total absence of deepfake-specific legislation until 2026, the Delhi High Court filled the vacuum through an expanding line of personality-rights decisions. Building on the constitutional foundation of privacy recognised in *K.S. Puttaswamy v. Union of India*,²¹ the Court

¹⁷ “IT Rules 2026 – Deepfake Regulation, Three-Hour Takedowns and AI Labelling Obligations”, Mondaq, available at: <https://www.mondaq.com/india/new-technology/1760554/it-rules-2026-deepfake-regulation-three-hour-takedowns-and-ai-labelling-obligations> (Last visited on 5 August 2026).

¹⁸ “IT Rules 2026”, iPleaders, available at: <https://blog.ipleaders.in/it-rules-2026/> (Last visited on 5 August 2026).

¹⁹ Digital Personal Data Protection Act, 2023.

²⁰ “ASCI Issues Draft Guidelines for Responsible Labelling of AI-Generated Content in Advertising”, Lexology, available at: <https://www.lexology.com/library/detail.aspx?g=eea2c4b2-6d46-4036-8869-d19aa3217c1c> (Last visited on 5 August 2026).

²¹ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

granted an ad-interim, in rem injunction to Amitabh Bachchan against the unauthorised commercial use of his name, voice, and image in a fraudulent lottery scheme,²² followed by a similarly omnibus injunction protecting Anil Kapoor against sixteen entities using AI, face-morphing, and deepfake tools to exploit his persona for commercial gain.²³ Subsequent orders have extended equivalent protection to Jaikishan Kakubhai Saraf ("Jackie Shroff"),²⁴ and, in September 2025, to Aishwarya Rai Bachchan against unauthorised use of her likeness across e-commerce platforms, chatbots, and AI-generated deepfake videos.²⁵

These "*Ashok Kumar*" (John Doe) orders are a powerful emergency remedy, but they are structurally a personality-rights tool, not a consumer-protection one: they vindicate the celebrity's proprietary interest in their own persona and only incidentally protect the consumer who was deceived by the fabricated endorsement. A consumer misled by a deepfake investment advertisement has no standing in these suits and must instead pursue relief, if at all, through consumer fora or cybercrime complaints mechanisms considerably slower than the speed at which deepfake advertising campaigns circulate and disappear.

C. Comparative Perspectives

India's fragmented approach contrasts with more codified transparency regimes elsewhere. Article 50 of the European Union's Artificial Intelligence Act imposes a direct, horizontal disclosure obligation: a deployer using AI to create content that resembles an existing person and would falsely appear authentic must disclose that the content is a deepfake, in a manner perceptible without technical tools, applicable from 2 August 2026 and enforceable with penalties of up to €15 million or three per cent of global turnover.²⁶ Unlike ASCI's advisory taxonomy, the EU obligation applies irrespective of intent to deceive and is backed by statutory penalties scaled to a company's revenue rather than a fixed rupee ceiling.

The United States has taken a narrower but more targeted route. The Federal Trade Commission's Trade Regulation Rule Regarding Consumer Reviews and Testimonials became effective on 21st October 2024 and forbids people from manufacturing, buying and selling any

²² *Amitabh Bachchan v. Rajat Nagi & Ors.*, 2022 SCC OnLine Del 4110.

²³ *Anil Kapoor v. Simply Life India & Ors.*, 2023 SCC OnLine Del 6914.

²⁴ *Jaikishan Kakubhai Saraf v. The Peppy Store & Ors.*, (2024) 2 HCC (Del) 253.

²⁵ *Aishwarya Rai Bachchan v. Defendant Nos. 1 to 20 & Ors.*, CS(COMM) 956/2025 (Delhi HC, order dated 9 September 2025).

²⁶ Article 50: Transparency Obligations for Providers and Deployers of Certain AI Systems, Regulation (EU) 2024/1689, available at: <https://artificialintelligenceact.eu/article/50/> (Last visited on 5 August 2026).

phony testimonials relating to celebrities.²⁷ Unlike India's CCPA Guidelines, which address endorser liability only through the soft obligation to hold a "genuine opinion," the FTC rule creates a specific, enforceable prohibition tailored to fabricated endorsements precisely the gap that Indian consumer law has yet to close explicitly for synthetic endorsers.

D. Statistical Analysis: The Scale and Pattern of Harm

Empirical data underscores why this gap matters. Nationally, the Indian Cyber Crime Coordination Centre recorded roughly 2.81 million cyber-fraud complaints in 2025, a 24 per cent increase over 2024, with reported losses of approximately ₹22,495 crore;²⁸ more than 92,000 "digital-arrest" and impersonation scams, many deploying AI-cloned voices and faces of law-enforcement or judicial officers were logged by law-enforcement sources in the same period.²⁹ Globally, Surfshark's analysis of the AI Incident Database found that investment-fraud deepfakes, typically using fabricated celebrity or executive endorsements distributed through social media, accounted for approximately USD 900 million, 57 per cent of all documented deepfake-related losses in the first three quarters of 2025 alone, with 83 per cent of such losses originating on social media platforms.³⁰ Sumsu's Identity Fraud Report similarly records deepfake fraud as now constituting 11 per cent of all fraud worldwide.³¹ These figures indicate that deepfake advertising is not a marginal or speculative harm but a rapidly scaling vector of financial fraud, concentrated precisely on the intermediary platforms and advertising formats for which current Indian consumer-protection penalties were calibrated in a pre-AI advertising ecosystem.

E. Critical Evaluation: Structural Gaps

In examining the issue at hand, four structural barriers can be noted. Firstly, there is no legislation in India that establishes a comprehensive definition of "deepfake advertisement" although the 2026 IT Rules use the term "synthetically generated information" for the purpose of meeting the standards of intermediaries and the Consumer Protection

²⁷ Federal Trade Commission, "Federal Trade Commission Announces Final Rule Banning Fake Reviews and Testimonials", available at: <https://www.ftc.gov/news-events/news/press-releases/2024/08/federal-trade-commission-announces-final-rule-banning-fake-reviews-testimonials> (Last visited on 5 August 2026).

²⁸ Supra note 2.

²⁹ "Your Voice, Your Face, Your Bank Account: AI Scams Are Evolving", available at: <https://www.dqindia.com/data-and-ai/ai-scams-india-2025-deepfake-identity-fraud-rs-22495-crore-12108304> (Last visited on 5 August 2026).

³⁰ "What Deepfake Fraud Actually Costs Businesses in 2025–2026", Veriff, available at: <https://www.veriff.com/fraud/deepfake-fraud-cost-2026> (Last visited on 5 August 2026).

³¹ Supra note, "Your Voice, Your Face, Your Bank Account" (n 30 above), citing Sumsu, Identity Fraud Report 2025–2026.

Act includes the term "misleading advertisement" for determining the liability of the endorser. Secondly, the amount of the penalty which the CCPA deems appropriate for repeat violations does not amount to more than 50 lac rupees, while losses resulting from deepfakes exceed thousands of crores, leading to almost no deterrent effect on the part of platforms and business owners profiting from deepfake commercials. Thirdly, although the 2026 IT Rules insist on labeling and fast removal of unlawful synthetic content, there is no requirement to verify an advertiser's identity in the context of deepfake advertising, which places such advertisements in the position of one of the most dangerous types of ads that can be published without effective surveillance. Lastly, ASCI's risk-based labeling framework, which is probably the best specific tool regarding advertising, continues to exist in a draft and non-binding version being applied just to ASCI's voluntary members and having no legal penalty.

FINDINGS

The analysis yields the following principal findings. First of all, India regulates deepfake advertisements only indirectly, through the interaction of general misleading-advertisement law, general intermediary due-diligence law, and general data-protection consent requirements, none of which was drafted with synthetic commercial endorsement in mind. Secondly, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 mark a genuine advance introducing labelling, provenance, and rapid takedown obligations, but their consumer-protection value depends on enforcement against paid advertising content specifically, an application not yet tested. Thirdly, judicial personality-rights litigation, while a valuable emergency remedy for named public figures, structurally excludes the deceived consumer as a party and cannot substitute for systemic regulation. Fourthly, the CCPA's penalty regime is disproportionately weak relative to the documented scale of deepfake-enabled financial fraud in India, estimated in the tens of thousands of crores annually. Lastly, comparative regimes in the European Union and the United States demonstrate that binding, penalty-backed disclosure obligations specifically targeting fabricated endorsements are both feasible and increasingly the international norm, whereas India's most advertising-specific response is the ASCI framework which remains voluntary.

RECOMMENDATIONS

Based on these findings, the article makes the following practical recommendations:

Firstly, the Consumer Protection Act, 2019 or the CCPA Guidelines, 2022

should be amended to define a “synthetic” or “deepfake advertisement” as a distinct category of unfair trade practice, triggered whenever an advertisement uses an AI-generated or AI-altered likeness, voice, or persona of a real or fictional endorser without clear, prominent disclosure.

Secondly, the Penalties under Section 21 of the Consumer Protection Act, 2019 should be revised for this category to a turnover-linked structure-mirroring the European Union's percentage-of-turnover model, rather than the current fixed ceiling of ₹50 lakh, which offers negligible deterrence to large advertisers or platforms.

Thirdly, the labelling taxonomy developed in ASCI's 2026 draft guidelines should be given statutory backing, either by incorporation into the CCPA Guidelines or by cross-reference in the Intermediary Guidelines, converting a currently voluntary, membership-limited code into a binding, universally applicable disclosure requirement.

Fourthly, the Intermediaries carrying paid financial, health, or investment advertisements should be required to verify advertiser identity before publication, analogous to political-advertising verification requirements, given that investment-fraud deepfakes constitute the largest single category of documented harm.

Fifthly, the three-hour and two-hour takedown windows introduced by the 2026 IT Rules should be explicitly extended, by clarificatory MeitY guidance, to cover fraudulent commercial deepfake advertisements reported by the Central Consumer Protection Authority, and not only content flagged through court or government order.

Lastly, the targeted AI-literacy campaigns should be directed at demographic groups disproportionately targeted by investment-fraud deepfakes, including elderly and first-time retail investors, who recur as a victim profile in reported cases.

CONCLUSION

Deepfake advertisements sit at the intersection of consumer protection, intermediary liability, and personality-rights law, yet no single Indian legal instrument treats them as a unified problem. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 and ASCI's draft labelling guidelines represent meaningful, overdue progress, but both remain either newly operational or non-binding, and neither is matched by a Consumer Protection Act penalty regime capable of deterring fraud of the scale now documented in India. As generative AI tools continue to fall in cost and rise in realism, the gap between the sophistication of synthetic advertising and the blunt instruments available to regulate it will widen unless Parliament and the

Central Consumer Protection Authority act to define, penalise, and pre-empt the deepfake advertisement as a distinct and rapidly scaling category of consumer harm.