



LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.348>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

MALICIOUS USE OF DEEPFAKES IN INDIA: LEGAL, TECHNOLOGICAL AND SOCIO-ECONOMIC CHALLENGES AND THE NEED FOR AN EFFECTIVE REGULATORY FRAMEWORK

Adv. Nilam Navanath Pawar¹

I. ABSTRACT

The rapid development of generative artificial intelligence has transformed the creation, manipulation and dissemination of audio-visual information. Deepfakes, broadly understood as synthetic or manipulated audio, images and videos capable of presenting fabricated persons, statements or events as authentic, have consequently become a significant legal and socio-economic concern. Although synthetic media has legitimate applications in education, entertainment, accessibility, research and creative expression, its malicious use can facilitate impersonation, financial fraud, defamation, misinformation, electoral manipulation, identity theft, non-consensual intimate imagery and child exploitation. This paper examines a central research question: whether India's existing legal and regulatory framework adequately addresses the distinct harms caused by malicious deepfakes while preserving constitutionally protected expression. It adopts a doctrinal and analytical approach to the Information Technology Act 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 as amended in 2026, the Bharatiya Nyaya Sanhita 2023, the Bharatiya Sakshya Adhinyam 2023, the Digital Personal Data Protection Act 2023, constitutional guarantees under Articles 14, 19 and 21, and relevant judicial developments concerning personality rights. The analysis finds that India now has an express regulatory framework for synthetically generated information, including intermediary obligations relating to unlawful synthetic content, prominent labelling and technical provenance mechanisms. However, legal protection remains dispersed across criminal, civil, evidentiary, data-protection and sector-specific regimes. Significant gaps persist in relation to electoral deception, cross-border investigation, attribution, authenticity of electronic evidence, rapid

¹ Research Scholar at ABMS Parishad's Yashwantrao Chavan Law College, Pune, Maharashtra (India). Email: nilamspwr@gmail.com

victim remedies and the coherent protection of personality rights. The paper therefore argues for a risk-based, harm-oriented and technology-neutral framework that differentiates legitimate synthetic expression from deceptive or malicious uses according to intent, foreseeable harm, scale of dissemination and intermediary involvement.

II. KEYWORDS

Deepfakes; Synthetically Generated Information; Intermediary Liability; Personality Rights; Digital Evidence.

III. INTRODUCTION

The digital environment has historically depended upon a basic assumption: that photographs, audio recordings and videos provide reasonably reliable evidence of events and statements. Generative artificial intelligence increasingly weakens that assumption. Modern AI systems can generate or manipulate voices, faces, photographs and videos in ways that may be difficult for ordinary viewers to distinguish from authentic material. The phenomenon commonly described as a "deepfake" is therefore not simply a technological development. It is a challenge to legal concepts of identity, consent, authenticity, reputation, evidence and responsibility.

The malicious deployment of deepfakes can take multiple forms. A person's face may be superimposed onto another body. A person's voice may be cloned to create an apparently authentic telephone instruction. A politician may appear to make a statement that was never made. A corporate executive may appear to authorise a financial transfer. A woman may be depicted in sexually explicit material without having participated in the underlying conduct. A fabricated recording may circulate during an election before verification is possible. The legal significance of these examples differs. A fraudulent voice recording used to obtain money raises questions of cheating and personation.

A fabricated sexual image may implicate privacy, dignity, obscenity, sexual offences and intermediary obligations. A false political video raises questions concerning freedom of expression, electoral integrity and the limits of governmental regulation.

The same technological process can therefore generate entirely different legal consequences depending upon context. India's initial response to deepfakes was necessarily indirect. The Information Technology Act 2000 predates contemporary generative AI. Its provisions concerning identity theft, cheating by personation, privacy and sexually explicit material were drafted without deepfake technology specifically in mind. The Information Technology Rules 2021 subsequently developed intermediary due-diligence obligations.

The regulatory position has now evolved. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026 introduced the concept of "synthetically generated information" and specific intermediary obligations. The amendment came into force on 20 February 2026. The definition covers audio, visual and audio-visual information artificially or algorithmically created, generated, modified or altered so that it appears real, authentic or true and depicts an individual or event in a manner likely to be perceived as indistinguishable from a natural person or real-world event.²

This development makes it necessary to reconsider the proposition that India lacks a regulatory response to deepfakes. The more accurate proposition is that India now possesses an express synthetic-media framework, but its relationship with criminal law, constitutional rights, civil remedies, evidence law, data protection and election law remains incompletely developed. The central argument of this paper is consequently that India requires neither a complete prohibition of deepfakes nor reliance exclusively upon existing criminal offences.

It requires a risk-based regulatory architecture in which liability is determined by the nature of the content, the harm caused or reasonably foreseeable, the intent of the

² Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, GSR 120(E), 10 February 2026, r 1(2) (providing that the amendment came into force on 20 February 2026).

actor, the scale of dissemination and the degree of involvement of the platform or AI provider.³

A. Research Problem

Despite the introduction of an express regulatory framework for synthetically generated information, Indian law continues to address malicious deepfakes through a dispersed combination of intermediary regulation, criminal law, evidence law, data protection, sector-specific legislation and judge-made personality rights. The central research problem is whether this fragmented framework can provide coherent, timely and proportionate remedies for distinct forms of deepfake harm while preserving legitimate synthetic expression protected by the Constitution.

Difficulties relating to attribution, electronic authenticity, cross-border investigation, rapid dissemination and the allocation of responsibility among creators, intermediaries and AI-service providers further complicate enforcement. The paper therefore examines how a technology-neutral and risk-based framework can integrate these areas of law and calibrate legal responsibility according to deception, intent, foreseeable harm, scale of dissemination and the degree of control exercised by relevant actors.

B. Research Objectives

The principal objectives of this research are:

1. To examine the adequacy and interrelationship of the existing Indian constitutional, criminal, intermediary, evidentiary, data-protection and sector-specific legal frameworks governing malicious deepfakes.
2. To identify the principal evidentiary, jurisdictional, attribution and enforcement difficulties arising in the investigation and adjudication of deepfake-related harms.
3. To analyse how regulation of deceptive synthetic media may protect privacy, dignity, reputation, electoral integrity and vulnerable persons

³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 2(1)(wa), as inserted by GSR 120(E). The consolidated text records the definition of SGI and the amendment by GSR 120(E).

while remaining consistent with constitutional protection of freedom of speech and expression.

4. To formulate a risk-based, harm-oriented and technology-neutral regulatory model that allocates proportionate responsibilities among content creators, intermediaries, social-media platforms and AI-service providers.

C. Research Questions

The paper examines five principal questions:

1. To what extent is India's existing legal and regulatory framework capable of addressing malicious deepfake activity?
2. What evidentiary, jurisdictional and attribution difficulties arise in investigating, proving and prosecuting deepfake-related conduct?
3. How should India regulate harmful synthetic media while preserving the constitutional protection of freedom of speech and expression?
4. What proportionate responsibilities should be imposed upon intermediaries, social-media platforms and AI-service providers in relation to the creation, dissemination, identification, labelling and removal of harmful synthetically generated information?
5. What legal and institutional reforms are necessary to establish a coherent, risk-based and technology-neutral framework for malicious deepfakes in India?

D. Research Questions

The paper examines five principal questions:

1. To what extent is India's existing legal framework capable of addressing malicious deepfake activity?

2. What evidentiary, jurisdictional and attribution difficulties arise in investigating and prosecuting deepfake-related offences?
3. How should India balance regulation of harmful synthetic media with the constitutional protection of freedom of speech and expression?
4. What responsibilities should be imposed upon intermediaries, social-media platforms and AI developers

E. Research Methodology

The research adopts a primarily doctrinal and analytical methodology. It examines constitutional provisions, statutes, delegated legislation, judicial decisions and official regulatory material. Secondary academic and institutional material is used to contextualise technological and socio-economic developments. The paper does not claim to provide a statistically comprehensive measurement of all deepfake incidents in India. Reported incidents are used illustratively and are distinguished from empirically established prevalence. Where an incident is based primarily on media reporting rather than a judicial finding, it is identified accordingly.

IV. UNDERSTANDING DEEPAKES AND THEIR MALICIOUS USES

A. Concept and Evolution

The expression "deepfake" derives from the use of deep-learning techniques to create or manipulate media. The technology has developed from relatively specialised face-swapping techniques into systems capable of generating realistic speech, images and video. Technically, contemporary synthetic media may involve generative adversarial networks, autoencoders, diffusion models, neural voice cloning and other machine-learning techniques. The legal question, however, does not depend upon the particular algorithm employed. The 2026 Indian regulatory framework appropriately moves towards a technology-neutral definition.

It refers to synthetically generated information rather than making the legality of the content dependent upon whether a particular algorithm, model or software application was used. This approach is preferable because technological terminology

changes rapidly. A statute that criminalised only "deepfake videos" could become obsolete as generative systems evolve.⁴

B. Legitimate and Malicious Uses

Synthetic media should not be equated automatically with unlawful content. AI-generated images may be used in films, advertisements, education and research. Voice synthesis can assist persons with disabilities. Digital reconstruction may have legitimate historical or artistic applications. Satire and parody may use synthetic representations of public figures as a form of political expression. The legal difficulty arises when synthetic media is presented deceptively or used to cause legally cognisable harm.

A useful distinction is therefore between:

1. disclosed synthetic expression;
2. undisclosed but relatively low-risk synthetic content;
3. deceptive synthetic content capable of significant harm; and
4. deliberately malicious synthetic content involving serious criminal, sexual, financial, electoral or public-order consequences.

This distinction should inform the level of regulatory intervention.

C. Malicious Applications

The principal forms of malicious deepfake use include:

1. **Impersonation and fraud:** A cloned voice or face may be used to impersonate a family member, government officer, business executive or financial professional.
2. **Identity theft:** A person's image, voice or identifying characteristics may be appropriated for fraudulent transactions.
3. **Political manipulation:** Synthetic media may create false endorsements, fabricated statements or false representations of political events.

⁴ Ibid.

4. **Defamation:** A person may be depicted committing an act or making a statement capable of lowering reputation.
5. **Non-consensual intimate imagery:** AI may create sexually explicit representations of a person without consent, even where no authentic intimate photograph of the person ever existed.
6. **Child exploitation:** Synthetic sexual representations involving children create particularly serious child-protection concerns.
7. **Corporate manipulation:** Deepfakes can be used to impersonate executives, manipulate employees or induce fraudulent transactions.
8. **Misinformation and public disorder:** Fabricated statements attributed to public officials may produce panic or influence public behaviour.

The legal system should therefore regulate harmful uses, rather than treating the technology itself as inherently unlawful.

V. THE DEEPPAKE THREAT LANDSCAPE IN INDIA

India's digital environment presents particular challenges because synthetic content can be distributed rapidly through multiple platforms and linguistic communities. A fabricated video need not remain on the platform where it first appeared. It can be downloaded, re-uploaded, cropped, translated, subtitled and distributed through encrypted messaging services. The 2025 MeitY explanatory material identified several risks associated with synthetic media, including misinformation, reputational injury, election manipulation, financial fraud, non-consensual intimate imagery and threats to information ecosystems.⁵

A. Electoral and Political Manipulation

The 2024 Indian general election provided a significant illustration of the political use of synthetic media. Manipulated videos involving actors Aamir Khan and Ranveer

⁵ Ministry of Electronics and Information Technology, Government of India, Explanatory Note: Proposed Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to Synthetically Generated Information (22 October 2025).

Singh circulated portraying them as criticising the government and supporting the Congress party.

The actors publicly denied the authenticity of the material. The incident was reported internationally as an example of AI-generated political manipulation during India's election. The legal importance of such incidents is not limited to whether a particular criminal offence is established. The speed of digital dissemination may create a temporal asymmetry: fabricated content can reach millions of people before the authentic source has an opportunity to respond. The appropriate legal response therefore requires both ex post remedies and ex ante transparency.⁶

B. Financial Fraud

Deepfake-enabled financial fraud may operate through cloned voices, manipulated video calls or fabricated instructions. In such cases the deepfake is a means rather than the ultimate offence. The BNS provision on cheating by personation is particularly relevant. Section 319 defines cheating by personation to include pretending to be another person or representing oneself or another as someone other than who they really are. The provision is technologically neutral and can therefore accommodate new methods of impersonation.

Synthetic intimate imagery presents one of the most severe forms of deepfake harm. The victim may have no connection to the underlying sexual content, yet the fabricated representation can produce real-world humiliation, harassment, reputational injury and social consequences. The 2026 IT Rules expressly recognise non-consensual intimate imagery within the category of unlawful synthetic information that intermediaries must address. The regulatory challenge is to provide a remedy sufficiently rapid to prevent repeated dissemination. Traditional criminal

⁶ Reuters, 'Deepfakes of Bollywood stars spark worries of AI meddling in India election' (22 April 2024). The incident should be treated as a reported case study rather than as a judicial finding concerning criminal liability.

prosecution alone is inadequate where the principal harm arises from continued online availability.⁷⁸

C. Women and Children

Deepfake sexual abuse has a gendered dimension. Women and girls may be disproportionately targeted because synthetic technology can transform ordinary publicly available photographs into sexually explicit material. POCSO is especially significant where children are involved. Sections 13 to 15 address use of children for pornographic purposes and related storage and possession conduct. The increasing ability to generate synthetic representations makes it necessary to ensure that child-protection law does not depend upon whether the image corresponds to an actual photographic event.⁹

VI. EXISTING INDIAN LEGAL AND REGULATORY FRAMEWORK

A. Information Technology Act, 2000

The IT Act remains the principal technology-related statute. Section 66C addresses identity theft, while section 66D concerns cheating by personation using a communication device or computer resource. These provisions can apply to deepfake-enabled fraud where the relevant statutory ingredients are established. Sections 67 and 67A may become relevant to obscene or sexually explicit material, while section 67B provides specific protection in relation to material involving children. The limitation is structural.

The IT Act regulates particular forms of unlawful conduct but does not create a general offence of "creating a deepfake". This is not necessarily a defect. Criminal law

⁷ Bharatiya Nyaya Sanhita 2023, s 319. The statutory text defines cheating by personation and prescribes punishment of imprisonment up to five years, or fine, or both.

⁸ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 3, as amended in 2026. The amended framework expressly identifies non-consensual intimate imagery among prohibited categories of synthetic information.

⁹ Protection of Children from Sexual Offences Act 2012, ss 13-15. India Code identifies sections 13, 14 and 15 as addressing use of children for pornographic purposes, punishment and storage of pornographic material involving children respectively.

should not automatically criminalise technological creation without reference to harm and culpability.¹⁰

B. Intermediary Rules and the 2026 SGI Framework

The new Rule 2(1)(wa) defines SGI as audio, visual or audio-visual information artificially or algorithmically created, generated, modified or altered through a computer resource so that it appears real, authentic or true and portrays an individual or event in a manner likely to be perceived as indistinguishable from a natural person or real-world event. Importantly, the Rules exclude routine good-faith editing, formatting, technical correction, accessibility-related modifications and similar activities where there is no material distortion or misrepresentation.

The framework also distinguishes between prohibited SGI and synthetic content that must be labelled. For certain prohibited categories, intermediaries must deploy reasonable and appropriate technical measures. These include child sexual exploitative material, non-consensual intimate imagery, obscene or sexually explicit content, false documents or electronic records and deceptive representations of natural persons or real-world events.^{11,12,13}

For other SGI, the framework requires prominent labelling and permanent metadata or another appropriate technical provenance mechanism to the extent technically feasible. This is a major shift from purely reactive content moderation towards a combination of prevention, transparency and provenance. Nevertheless, several questions remain. First, automated detection will not always be accurate. Secondly, technical provenance can be removed when content moves outside controlled

¹⁰ Information Technology Act 2000, ss 66C, 66D, 67, 67A and 67B.

¹¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 2(1)(wa), as amended by GSR 120(E).

¹² Ministry of Electronics and Information Technology, Government of India, Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. The official FAQ identifies routine good-faith editing, formatting, technical correction and accessibility-related uses as exclusions where they do not materially alter or misrepresent the underlying content.

¹³ Information Technology Rules 2021, r 3(3)(a)(i), as inserted by the 2026 amendment. The consolidated text identifies CSAM, non-consensual intimate imagery, obscene or sexually explicit material, false documents/electronic records and deceptive representations of persons or real-world events among the specified categories.

platforms. Thirdly, determining whether a representation is "likely to deceive" may involve contextual judgments that cannot always be automated. Fourthly, over-compliance could encourage platforms to remove lawful satire, political criticism or artistic content.¹⁴

C. Bharatiya Nyaya Sanhita, 2023

The BNS provides several provisions that may be relevant to deepfake-related conduct. Section 318 addresses cheating, while section 319 addresses cheating by personation. Section 319 expressly covers representation as another person and applies whether the person impersonated is real or imaginary. The BNS also contains provisions concerning forgery, criminal intimidation and defamation that may apply depending upon the facts.

The principal strength of the BNS is technological neutrality. The principal limitation is that prosecutors must still establish the ingredients of the specific offence. Thus, a fabricated video does not become cheating merely because it is fabricated. There must be deception and the other elements of the offence. Similarly, a manipulated video does not automatically constitute defamation. The legal requirements of the applicable defamation provision must be satisfied.¹⁵

D. Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS is relevant primarily through investigation, search, seizure, production of electronic evidence, procedural safeguards and jurisdiction. Deepfake investigations may involve devices, cloud accounts, platform logs, metadata and communications located in different jurisdictions. The effectiveness of substantive offences therefore depends substantially upon procedural capacity. Cross-border evidence remains particularly challenging. A domestic investigation may identify a platform account without obtaining timely access to the underlying subscriber information or server records.¹⁶

¹⁴ Information Technology Rules 2021, r 3(3)(a)(ii), as inserted by the 2026 amendment.

¹⁵ Bharatiya Nyaya Sanhita 2023, s 319.

¹⁶ Bharatiya Nagarik Suraksha Sanhita 2023.

E. Bharatiya Sakshya Adhiniyam, 2023

The BSA is central to the evidentiary dimensions of deepfakes. Section 61 provides that electronic or digital records cannot be rejected merely because they are electronic and provides that they have the same legal effect as other documents subject to section 63. Section 63 governs admissibility of electronic records. Deepfakes demonstrate why admissibility and authenticity must be analytically separated. A video can satisfy formal requirements for admission while still being a manipulated representation of an event. The law should not assume that visual realism establishes factual authenticity.¹⁷

F. Digital Personal Data Protection Act, 2023

The DPDP Act regulates processing of digital personal data and recognises the individual's interest in protection of personal data. Deepfakes can involve the processing of facial images, voices and other information relating to identifiable individuals. However, data protection and personality rights are conceptually distinct. A person may suffer dignitary or reputational harm from synthetic content even where a particular data-protection provision is not applicable. The DPDP framework should therefore operate alongside, rather than replace, privacy, personality and criminal-law remedies.¹⁸

G. Indecent Representation of Women (Prohibition) Act, 1986

The Act seeks to prohibit indecent representation of women through advertisements, publications, writings, paintings, figures or other forms. Its relevance to deepfakes is apparent, but its formulation predates generative AI. A future reform should clarify its relationship with synthetic sexual imagery rather than leaving courts to stretch

¹⁷ Bharatiya Sakshya Adhiniyam 2023, ss 61-63. Section 61 recognises the legal effect of electronic or digital records subject to s 63, while s 63 provides the conditions for admissibility of electronic records.

¹⁸ Digital Personal Data Protection Act 2023, Act 22 of 2023. The Act recognises the right of individuals to protect their digital personal data while permitting lawful processing. The commencement provisions have been brought into effect in stages through government notification.

decades-old statutory language to accommodate technologies that Parliament could not have anticipated.¹⁹

H. POCSO Act, 2012

Sections 13 to 15 of POCSO address use of children for pornographic purposes and related possession/storage conduct. The emergence of AI-generated child sexual material raises difficult questions concerning the relationship between actual abuse and synthetic representation. The law must protect children without allowing technological fiction to become a loophole for exploitation.²⁰

I. Representation of the People Act, 1951

The RPA regulates elections, corrupt practices and election offences. The problem is that synthetic political content can cause electoral harm without necessarily fitting existing categories of corrupt practice. A fabricated statement by a candidate may be deceptive but not necessarily amount to a statutory corrupt practice under the existing formulation. Election law therefore requires additional safeguards specifically addressing materially deceptive synthetic political content.²¹

J. Copyright Act, 1957

Copyright may become relevant where deepfake creation involves copying protected photographs, films, recordings or other works. However, copyright is not a complete solution. A victim may have no copyright ownership over an ordinary photograph of themselves, while their privacy, dignity or personality may nevertheless be infringed. Copyright should therefore remain a supplementary rather than primary deepfake remedy.²²

¹⁹ Indecent Representation of Women (Prohibition) Act 1986, long title and ss 3-4. India Code describes the Act as legislation prohibiting indecent representation of women through advertisements, publications, writings, paintings, figures or other forms.

²⁰ Protection of Children from Sexual Offences Act 2012, ss 13-15.

²¹ Representation of the People Act 1951, long title. The Act provides for the conduct of elections and regulates corrupt practices and offences in connection with elections.

²² Copyright Act 1957.

K. Consumer Protection Act, 2019

Deepfake advertisements may create consumer-law issues where synthetic representations are used to falsely endorse products or services. The Consumer Protection Act can therefore supplement criminal and intermediary law where deceptive advertising or unfair trade practices affect consumers.²³

VII. CONSTITUTIONAL AND HUMAN RIGHTS DIMENSIONS

A. Article 21 and Privacy

The constitutional right to privacy is foundational to the regulation of deepfakes.

In *Justice KS Puttaswamy (Retd) v Union of India*, the Supreme Court recognised privacy as a fundamental right and closely connected privacy with dignity, autonomy and control over personal information. The Court's analysis is particularly relevant to deepfakes because synthetic identity manipulation involves appropriation of aspects of an individual's personality. A person's face or voice may be publicly visible, but public availability does not necessarily amount to unlimited consent for synthetic manipulation.²⁴

B. Dignity and Reputation

Deepfakes can affect reputation independently of physical or financial harm.

In *Subramanian Swamy v Union of India*, the Supreme Court recognised reputation as an aspect of Article 21 and considered the relationship between reputation and freedom of speech. A fabricated video depicting a person engaging in criminal, immoral or socially unacceptable conduct may therefore create a legally significant reputational injury.²⁵

²³ Consumer Protection Act 2019.

²⁴ *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1. The Supreme Court recognised privacy as a fundamental right and connected it with dignity, autonomy and informational control.

²⁵ *Subramanian Swamy v Union of India* (2016) 7 SCC 221. The Supreme Court considered reputation as an aspect of Article 21 and examined the constitutional relationship between reputation and freedom of speech.

C. Personality Rights

Indian courts have increasingly developed personality-rights jurisprudence.

In *Anil Kapoor v Simply Life India*, the Delhi High Court restrained misuse of the actor's name, likeness, image, voice and personality, including misuse through AI, machine learning, deepfakes and face morphing. The Court's order expressly referred to AI-generated images and videos, including fake pornographic material.^{26, 27}

In *Arijit Singh v Codible Ventures LLP*, the Bombay High Court, while granting ex parte ad-interim relief, recognised prima facie that making AI tools available to convert a voice into that of a celebrity without permission constitutes a violation of personality rights. The Court specifically addressed AI voice models, voice-conversion tools, synthesised voices, generative AI and deepfake technologies used to appropriate the plaintiff's identifiable personality attributes."²⁸

"Read together with the Delhi High Court's decision in *Anil Kapoor v Simply Life India*, the Bombay High Court's ruling in *Arijit Singh* demonstrates that more than one Indian High Court has extended judge-made personality-rights protection to unauthorised uses involving artificial intelligence. These decisions reinforce the emergence of a civil remedy notwithstanding the absence of a comprehensive statutory personality-rights regime.

D. Article 19(1)(a)

The regulation of deepfakes directly affects freedom of speech and expression. Not every synthetic representation is harmful. Political satire, parody, artistic expression and fictional works may involve fabricated representations of public figures. A blanket prohibition could therefore be constitutionally overbroad.

The appropriate approach is to distinguish between:

1. deception and parody;
2. undisclosed impersonation and disclosed fiction;

²⁶ *Anil Kapoor v Simply Life India*, 2023 SCC OnLine Del 6914 (Delhi High Court, 20 September 2023).

²⁷ *Anil Kapoor v Simply Life India* (Delhi High Court, 30 April 2024).

²⁸ *Arijit Singh v Codible Ventures LLP*, 2024 SCC OnLine Bom 2445 (Bombay High Court, 26 July 2024).

3. political criticism and fraudulent political representation;
4. artistic transformation and harmful sexual fabrication.

E. Article 19(2)

Article 19(2) permits reasonable restrictions on speech on specified grounds. Deepfake regulation may implicate defamation, public order, incitement, decency or morality and other recognised grounds depending upon the conduct. However, the existence of a legitimate governmental objective does not eliminate the requirement of proportionality. A regulatory provision should therefore be sufficiently precise to distinguish serious harms from legitimate synthetic expression.²⁹

F. Article 14

Article 14 becomes relevant where the regulatory framework classifies platforms, creators or synthetic content. Large social-media platforms capable of algorithmically amplifying material may legitimately be subject to greater obligations than individual users. However, the classification must bear a rational relationship to the regulatory objective.³⁰

VIII. CASE STUDIES

A. Aamir Khan and Ranveer Singh Election Videos

The manipulated videos involving Aamir Khan and Ranveer Singh during the 2024 general election illustrate the political risks of synthetic media. The actors denied making the statements attributed to them, and the videos were reported as manipulated. The incident is significant because it demonstrates the speed with which a fabricated political endorsement can enter the electoral information environment. The case does not, by itself, establish that a particular individual committed a statutory offence. It is therefore important to distinguish the existence and circulation of the manipulated material from proof of criminal responsibility.³¹

²⁹ Constitution of India, arts 19(1)(a) and 19(2).

³⁰ Constitution of India, art 14.

³¹ Reuters, 'Deepfakes of Bollywood stars spark worries of AI meddling in India election' (22 April 2024).

B. Anil Kapoor

The Anil Kapoor litigation provides a judicially verified example of misuse of personality through AI and deepfake technology. The Delhi High Court recorded allegations involving AI-generated images, videos, face morphing and fake pornographic material and granted injunctive protection over the plaintiff's name, likeness, image, voice and persona. The case demonstrates the usefulness of civil injunctions, particularly where the principal objective is stopping continuing dissemination.³²

C. Arijit Singh

The *Arijit Singh* litigation involved unauthorised use of the singer's personality attributes and AI-enabled voice conversion. In an ex parte ad-interim order dated 26 July 2024, the Bombay High Court held, on a prima facie assessment, that making AI tools available to convert a voice into that of a celebrity without permission violates the celebrity's personality rights. The Court also restrained unauthorised exploitation through AI voice models, voice-conversion tools, synthesised voices, generative AI, deepfakes and related technologies. The case demonstrates an important extension of personality-rights protection from direct misuse of celebrity attributes to AI platforms and tools facilitating such appropriation.³³

D. Jaya Bachchan

In *Jaya Bachchan v Bollywood Bubble Television*, the Delhi High Court restrained unauthorised use of the plaintiff's name, image, likeness, signature and voice through AI, generative AI, machine learning, deepfakes and face morphing. The case illustrates the development of Indian personality-rights jurisprudence in the absence of a comprehensive statutory personality-rights regime.³⁴

³² Anil Kapoor v Simply Life India, 2023 SCC OnLine Del 6914 (Delhi High Court, 20 September 2023); see also subsequent orders in the same proceedings.

³³ Arijit Singh v Codible Ventures LLP, 2024 SCC OnLine Bom 2445 (Bombay High Court, 26 July 2024).

³⁴ Jaya Bachchan v Bollywood Bubble Television (Delhi High Court, 10 November 2025).

IX. SUGGESTIONS AND RECOMMENDATIONS

India's emerging regulation of synthetically generated information should be developed through a risk-based model that supplements, rather than replaces, the existing criminal, intermediary, evidentiary and constitutional framework. Such a model should distinguish lawful synthetic expression from deceptive or harmful uses and should calibrate obligations according to the seriousness and foreseeability of harm, the intention of the actor, the scale of dissemination and the degree of technical or editorial control exercised by the relevant intermediary or AI-service provider.

1. **Tiered Regulation According to Harm:** The existing distinction between prohibited and permissible synthetically generated information should be developed into a clearer tiered regulatory structure. Disclosed and comparatively low-risk synthetic content should principally attract transparency, labelling and provenance requirements. Deceptive content presenting a material risk of reputational, financial or informational harm should attract enhanced complaint-handling, traceability and preservation obligations. High-risk or unlawful content, including non-consensual intimate imagery, child sexual exploitative material, fraudulent impersonation, false electronic records and materially deceptive representations of persons or events, should remain subject to expedited preventive and remedial measures in accordance with applicable law. Liability should depend upon the conduct and culpability of the relevant actor rather than upon the mere use of generative technology.
2. **Statutory Protection of Personality Rights:** India should consider a narrowly framed statutory civil remedy against unauthorised deceptive or exploitative use of an identifiable person's name, image, likeness, voice or other distinctive attributes through synthetic media. Such a provision could provide for injunctive relief and appropriate monetary remedies while consolidating principles presently developed substantially through judicial decisions. Any statutory right should contain safeguards for legitimate news reporting, public-interest communication, criticism, satire, parody, artistic expression and

consensual or sufficiently transformative uses so that personality protection does not become an excessive restriction upon lawful expression.

3. **Electoral Safeguards for Materially Deceptive Synthetic Content:** Election law should expressly address materially deceptive synthetic campaign content capable of falsely representing the identity, speech or conduct of a candidate or other identifiable person in an electoral context. The Representation of the People Act 1951 or appropriate election rules could provide statutory disclosure requirements for AI-generated or materially altered campaign material, together with an expedited mechanism for verification, correction or other lawful remedial action during the election period. Clearly disclosed satire, parody and legitimate political criticism should remain distinguishable from deceptive impersonation. Such reform would place existing administrative transparency measures concerning AI-generated campaign material on a clearer statutory footing.
4. **Authentication Protocols for Electronic and Synthetic Evidence:** The evidentiary framework should be supplemented by standard protocols for material suspected of being synthetically generated or manipulated. Consistently with sections 61 to 63 of the Bharatiya Sakshya Adhiniyam 2023, investigative and forensic practice should preserve the original electronic file wherever available, record its source and acquisition process, calculate and document cryptographic hash values, preserve relevant metadata and platform records, maintain an auditable chain of custody and record the methodology used in forensic examination. Provenance information, labels or metadata should constitute relevant indicators of authenticity but should not automatically be treated as conclusive. Where authenticity is genuinely disputed, appropriately qualified forensic evidence may assist the court in distinguishing the formal admissibility of an electronic record from the separate question whether its apparent audio-visual content authentically represents the underlying event.

X. CONCLUSION

Deepfakes expose a structural challenge for contemporary law. The difficulty is not merely that artificial intelligence can fabricate convincing media. The deeper problem is that the legal system must determine when fabrication becomes deception, when deception becomes legally cognisable harm, and who should bear responsibility for preventing or remedying that harm. India's regulatory position has changed significantly. The 2026 amendments to the IT Rules represent an important transition towards explicit governance of synthetically generated information. The framework recognises prohibited categories, labelling requirements and provenance mechanisms. At the same time, the new framework cannot by itself resolve all questions.³⁵

Criminal law remains fragmented. Civil personality-rights protection has developed substantially through judicial decisions but remains largely judge-made. Election law does not comprehensively address synthetic political communication. Evidence law recognises electronic records but does not make audiovisual authenticity self-evident. Cross-border investigation remains difficult. Victims of intimate deepfakes require remedies substantially faster than conventional litigation. The constitutional dimension makes a blanket prohibition inappropriate. Synthetic media may be used for satire, art, political commentary, education and accessibility. The State must therefore distinguish harmful deception from protected expression.

The most appropriate Indian response is consequently a risk-based, harm-oriented and technology-neutral regulatory framework. India therefore requires a regulatory framework capable of protecting privacy, dignity, reputation, children, women, electoral integrity and economic interests while preserving constitutionally protected expression and technological innovation. The success of such a framework will ultimately depend not on the breadth of prohibition but on the precision with which law distinguishes legitimate synthetic expression from harmful synthetic deception

³⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, GSR 120(E).

XI. BIBLIOGRAPHY

A. Primary Indian Legislation

1. Bharatiya Nagarik Suraksha Sanhita 2023.
2. Bharatiya Nyaya Sanhita 2023.
3. Bharatiya Sakshya Adhiniyam 2023.
4. Constitution of India.
5. Consumer Protection Act 2019.
6. Copyright Act 1957.
7. Digital Personal Data Protection Act 2023.
8. Indecent Representation of Women (Prohibition) Act 1986.
9. Information Technology Act 2000.
10. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, as amended, including the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026.
11. Protection of Children from Sexual Offences Act 2012.
12. Representation of the People Act 1951.

B. Indian Judicial Authorities

1. *Anil Kapoor v Simply Life India* (Delhi High Court, 20 September 2023).
2. *Anil Kapoor v Simply Life India* (Delhi High Court, 30 April 2024).
3. *Arijit Singh v Codible Ventures LLP* 2024 SCC OnLine Bom 2445 (Bom HC, 26 July 2024).
4. *Jaya Bachchan v Bollywood Bubble Television* (Delhi High Court, 10 November 2025).
5. *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
6. *Pooja Ramesh Singh v Jammu and Kashmir Bank Ltd*, 2026 INSC 668.
7. *Shreya Singhal v Union of India* (2015) 5 SCC 1.
8. *Subramanian Swamy v Union of India* (2016) 7 SCC 221.

C. Government And Regulatory Material

1. Ministry of Electronics and Information Technology, Government of India, *Explanatory Note: Proposed Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to Synthetically Generated Information* (22 October 2025).
2. Ministry of Electronics and Information Technology, Government of India, *Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*.
3. Ministry of Electronics and Information Technology, Government of India, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, GSR 120(E), 10 February 2026*.
4. Election Commission of India, official directions and advisories concerning responsible use of social media and synthetic/AI-generated content during elections.