INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A CRITICAL ANALYSIS OF DEEPFAKE PERSONALITIES AND VOICE CLONING: LEGAL CHALLENGES AND REGULATORY GAPS IN INDIA UNDER THE BACKDROP OF ARTIFICIAL INTELLIGENCE

AUTHOR - SIMMI PRAKASH* & DR. NIKUNJ SINGH YADAV**

* LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY, DEHRADUN, UTTARAKHAND, INDIA

** ASSISTANT PROFESSOR, LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY, DEHRADUN, UTTARAKHAND, INDIA

BEST CITATION - SIMMI PRAKASH & DR. NIKUNJ SINGH YADAV**,** A CRITICAL ANALYSIS OF DEEPFAKE PERSONALITIES AND VOICE CLONING: LEGAL CHALLENGES AND REGULATORY GAPS IN INDIA UNDER THE BACKDROP OF ARTIFICIAL INTELLIGENCE**,** INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (1) OF 2026, PG. 966-972, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/JIAW2275

1. Abstract

The sudden explosion in the development of artificial intelligence has led to the development of deepfakes as well as voice cloning technology that can reproduce the face, voice and behavioural qualities of an individual with a high degree of realism. While use of these technologies has legitimate applications, the misuse of these technologies has led to identity theft, reputational damage, non-consensual explicit content and sophisticated financial fraud. In India, the lack of a separate statutory framework for regulation of synthetic media has led to serious regulatory gaps as dependence is on scattered provisions of the Information Technology Act, the Indian Penal Code and the evolving data protection norms. 1

This paper adopts a doctrinal research methodology on the basis of statutes, judicial precedents, policy reports and academic literature to analyze the legal implications of deepfake personalities and voice cloning. It assesses how far there is any adequacy within the current Indian legislation in tackling the issues related to violation of right of privacy, personality rights, defamation and impersonation, failures in existence of enforcement structural loopholes and accountability in platforms.2

The study finds that existing legal remedies are reactive and technologically deficient, especially in relation to consent, harm in real time and cross-platform dissemination of harm. In popular culture Voice cloning creates even more risks as it facilitates targeted impersonation and financial trickery that prey on trust relationships.3 In this context the public health legal advocacy piece calls for a specialised legal framework which recognises facial likeness and voice as protected attributes, including a requirement to disclose AI-generated content and incorporate criminal offence against malicious synthetic media. Such regulation is necessary to protect the constitutional right to privacy, dignity and reputation in a balance with innovation and free expression.

2. Introduction

Artificial intelligence has revolutionized digital content creation with the ability to create hyper-realistic synthetic media that is commonly known as deepfakes. Deepfakes makes use of machine learning models, specifically generative adversarial networks, that can be used to manipulate or create

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

audio-visual content in a way that makes them appear authentic. A related technological development is voice cloning, which enables the reproduction of a person's speech patterns and tone based on minimum input of audio. Together these technologies make it much easier than AI systems to fake identities, raising complex legal questions around consent, likeness ownership and responsibility for abuse of misuse.1[2162]

Recent incidents show that deepfakes can be used to generate non-consensual explicit content, impersonate public figures and scams that are based on voice. Such practices pose a threat to the constitutional right to privacy recognised by the Supreme Court of India and to the right of reputation as a component of personal dignity.4 They also pose a risk to experiencing democratic discourse and persuasive misinformation as well as a loss of trust in digital evidence, often called the "liar's dividend."2

The central problem, which is researched in this paper, is whether the existing legal framework in India is sufficient to govern the deepfake personality and voice clones. At present, victims are left to draw from scattered provisions relating to impersonation, cheating, obscenity and data misuse, which were not intended with AI-generated harms in mind.5 This leaves them unsure of liability, jurisdiction and platform responsibility.

The objectives of this study are threefold: firstly, to look into the technological and legal elements of deepfakes and synthetic voices; secondly, to analyse the applicability and limitations of the current laws in India and, finally, to suggest an overall coherent regulatory framework. The research is driven by the following questions: set out are (i) what are the legal rights infringed by deepfakes and cloned voices; (ii) to what extent are existing statutes remedial; and (iii) is a tailored deepfake law needed?

The scope of the paper is restricted to the Indian legal context making selective comparative references. It focuses on the malicious uses of synthetic media and does not look in depth at technical development.

3. Research Methodology

This study is based on doctrinal research methodology based on a qualitative analysis of secondary sources. The research is based on statutory provisions such as the Information Technology Act, 2000, relevant provisions of the Indian Penal Code, the Digital Personal Data Protection Act, 2023 and the Intermediary Guidelines, 2021.[5–7] Judicial precedents recognizing the existence of the right to privacy and protection of reputation are analysed with the view is to assess their applicability to synthetic media harms.4

In addition, the paper focuses on the examination of scholarly literature, policy reports and documented case studies on deepfake misuse and voice cloning fraud.13 Comparative regulatory approaches and the international policy dialogue are addressed in order to identify best practices and normative standards.2

The doctrinal method helps to systematically examine the currently existing legal norms and identify the gaps and inconsistencies and thereafter make recommendations on an ideal regulatory framework for deepfakes and voice cloning in India.

4. Conceptual Framework

4.1 Deepfake Technology

Deepfakes are a type of synthetic media produced with artificial intelligence that makes the realistic copy of a person's facial features, expressions and voice. The technological basis for deepfakes is generative adversarial networks (GANs), which work with a double

[2162] Shinu Vig, *Regulating Deepfakes: An Indian Perspective*, 17 J. STRATEGIC SECURITY 70 (2024).
Vig-RegulatingDeepfakes-2024-1
Todd C. Helmus, *Artificial Intelligence, Deepfakes, and Disinformation: A Primer* (RAND Corporation, 2022).
HELMUS-ArtificialIntelligenceDe…
Jon Bateman, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios* (Carnegie Endowment for International Peace, 2020).
Bateman-ScenariosTargetingIndiv…

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

architecture of neural networks, where one part of the network is responsible for creating fake content while another part is responsible for testing whether this content is fake or not. Through the process of iterative training, the system produces outputs that are in turn becoming indistinguishable from real audio-visual material. 8

Deepfake production generally includes methods like swapping of a face, facial reenactment and synthetic generation of audio. These methods enable the superimposition of the face of one person onto the body of another, the transfer of facial expressions from a source video to a target facial expression as well as the artificial reconstruction of speech patterns. Although there are legitimate uses for such technologies from the fields of entertainment, digital communication and accessibility, there are also problematic uses that could fabricate events and manipulate public perception. The increasing accessibility and realism of these tools pose a challenge to the legal systems that traditionally use audio-visual content as credible evidence. 9

4.2 Voice Cloning and Identity Theft?

Voice cloning is a type of synthetic media and a more specific example of how synthetic media works we replicate speech of individual through a machine learning model using limited audio samples of that individual. Contemporary systems are able to produce real time speech very similar to the tone, accent and inflection of emotion, making them hard to detect.10

The legal significance of voice cloning is that it can be used to facilitate identity theft, impersonation and financial fraud. Deepfake voice calls can be used to trick employees into authorising financial transfers, manipulate individuals into providing confidential information and take advantage of trust-based relationships. Such attacks can be especially effective because they have a sense of urgency and authenticity that pure phishing[2163] has for lack thereof.10 Additionally, a possibility for the introduction of realistic audio recordings leads to serious concerns regarding evidentiary standards as it can be seen that synthetic speech can be presented as evidence in legal or administrative proceedings and consequently it complicates the standards of authentication and attribution.

5. Legal Issues Arising from Deepfakes

5.1 Violation of the Right to Privacy

Creation and dissemination of deepfake content without consent will therefore amount to a direct infringement of the right to privacy recognised as a fundamental right by the Supreme Court in Justice K.S. Puttaswamy v. Union of India.11 Deepfakes have been unauthorised use of bio-metric attributes like facial features and voice that belong to the area of information and bodily privacy. Such misuse, in addition to violating personal autonomy, also causes reputation and psychological harm. Existing privacy jurisprudence, however, does not clearly speak to AI-generated identity manipulation, leaving uncertainty as to the extent of remedies.

5.2 Rights to Personality and Rights to Publicity

Deepfakes often include the unauthorised commercial or non-commercial use of a person's name, image or likeness. Indian courts have thus acknowledged personality rights as an extension of right to privacy and proprietary interest in the identity of a person. The use of synthetic media with celebrities in advertisements or fake videos is misappropriation of the publicity right and economic exploitation. The lack of a coherent statutory scheme for personality rights regime in India leads to a considerable amount of

[2163] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
Information Technology Act, 2000, §§ 66C, 66D, 67, 72.
Indian Penal Code, 1860, §§ 419, 420, 499, 500.
Digital Personal Data Protection Act, 2023; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

8. Todd C. Helmus, *Artificial Intelligence, Deepfakes, and Disinformation: A Primer* (RAND Corporation, 2022). HELMUS-ArtificialIntelligenceDe…
9. Shinu Vig, *Regulating Deepfakes: An Indian Perspective*, 17 J. STRATEGIC SECURITY 70 (2024).

ambiguity in determining the liability and damages.

5.3 Defamation and False Light

Deepfakes have potential to defame people by putting false statements or conduct in their name which result in loss of reputation to that person (civil/defamation). Unlike defamatory content produced traditionally, synthetic audio-visual material looks authentic and is therefore more persuasive to viewers. The related idea of false light takes on relevance in the case of deepfakes that depict individuals in misleading situations not in the absence of specifically defamatory utterances, thus raising the extent of reputational damage.

5.4 Cybercrime, Fraud and Identity Theft

Deepfakes help in facilitating cyber offences as they can simulate another individual to include the digital identity of another. Voice cloning scams can circumvent traditional authentication mechanisms and trick victims into making money transactions.10 While there are current legal frameworks in place to deal with cheating and impersonation issues, they are not fully sufficient to deal with automated manufacturing of and the rapid dissemination and cross-border nature of synthetic media.

5.5 Gendered Harm and Deepfake Porn.

A significant percentage of malicious deepfake content is made up of the non-consensual explicit imagery of women. Such material violates dignity, privacy and bodily autonomy and often result in severe psychological and social consequences.9 Deepfake pornography is a form of technology-facilitated gender-based violence that is inadequately addressed by current provisions of the law governing obscenity and cybercrime, which were not meant to regulate the use of AI-generated sexual imagery created without consent.

6. Indian Legal Framework: A Critical Analysis

Indian legal framework covers deepfake related harms by way of combination of statutory provisions, none of which were created with the concept of synthetic media in mind. The Information Technology Act, 2000 has provisions relating to identity theft, cheating by personation, publication of obscene material and breach of confidentiality. 12 These sections, while providing limited means of remedy, fail to address for AI-generated biometric replication or impersonation in real-time.

Similarly, the Indian Penal Code has provisions for dealing with cheating, impersonation and defamation that may be used in relation to the misuse of deepfakes.13 However, these provisions exist on the basis of a traditional understanding of deception and they do not sufficiently cover the technological complexity, scale and speed of synthetic media dissemination.

Copyright law does provide protection for original works, however, copyright does not clearly recognise an individual's facial likeness or voice as a form of protectable subject matter. This leaves a regulatory gap in cases with regard to the unauthorised synthetic replication of identity for commercial purposes.

The Digital Personal Data Protection Act, 2023 provides a consent-based framework for the processing of personal data and may apply where facial images or voice samples are used without authorisation.14 Thus, again, the statute does not curtail AI generated outputs and provides no remedies for damage to repute due to deepfakes. The Intermediary Guidelines, 2021 include due diligence requirements on platforms to remove illegal content upon notice, however, platforms are on a reactive model and not on a proactive detection and labelling of synthetic media.14[2164]

Taken together these laws send the message of a fractured and reactionary mode of regulation:

[2164] Vig-RegulatingDeepfakes-2024-1

8. Jon Bateman, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios* (Carnegie Endowment for International Peace, 2020).

Bateman-ScenariosTargetingIndiv…

9. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
10. Information Technology Act, 2000, §§ 66C, 66D, 67, 72.
11. Indian Penal Code, 1860, §§ 419, 420, 499, 500.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

India does not yet have a dedicated statutory framework accounting for facial likeness and voice as a protected attributes and holds platforms accountable and requires criminal liability for the malicious creation and distribution of deepfakes.1

7. Case Studies

7.1 Rashmika Mandanna Deepfake

The spread of a deepfake video featuring Rashmika Mandanna highlighted the existence of synthetically produced visual resemblance and how it be easily and quickly spread through mediums in digital spaces without consent. The video, produced using face-swapping technology, did a lot of damage before proper takedown measures could be taken. Such incidents in fact illustrate the rapidity with which synthetic media can do irreversible damage, and the limitations associated with reactive legal responses. 9

Legally, the misuse engages the right to privacy, the rights to personality and dignity. The unauthorised use of the image of a celebrity is also an interference with the commercial value of endorsements and brand associations, and so implicates economic rights. The case brings out the lack of a statutory framework recognising facial likeness as a protected attribute and proactive intermediary accountability.15

7.2 Aishwarya Rai AI Image Misuse

AI generated images of Aishwarya Rai in manipulated and promotional settings have been circulated largely without authorisation. Such synthetic reproductions blur the lines between original and fraudulent visual content, raising the questions of ownership and control over digital identity.

The misuse is misappropriation of publicity rights and economical exploitation of an identity. It also reveals the gap in the protection afforded by copyright legislation that protects original work, but that gap is not explicit in the case of biometric identity. This leaves a regulatory gap in which synthetic imitation of likeness for commercial purposes is not protected by traditional intellectual property protection.15

7.3 Arijit Singh Voice Cloning Risk

Advances in AI-generated music have allowed for the imitation of a singer's vocal tone and style with machine learning models that are trained using recordings publicly available online. In the case of Arijit Singh, such voice cloning, results in the risk of unauthorised songs being distributed in the name of Arijit Singh.

This raises complex legal issues in respect of moral rights, economic rights - and ownership of voice identity. As opposed to traditional copyright infringement, voice cloning does not recreate a particular sound recording, but recreates distinctive vocal qualities. Lack of statutory protection of voice as a personality attribute leaves performers vulnerable to economic loss and damage to their reputation.[10]

These case studies collectively show that deepfakes and voice clones pose a threat to both the personal dignity and commercial value of identity and that this requires those biometric features to be legally recognised as a protectable right.

8. Comparative Jurisdictions

Different jurisdictions have implemented regulatory strategies towards the coping with deepfakes.

In the US, multiple states, including California and Texas, have introduced laws that make it a criminal offense to nefariously distribute deepfakes that are designed to affect the course of elections, or to create non-consensual explicit content. It is with these considerations in mind that these laws recognise the potential of the use of synthetic media to undermine democratic processes and the individual's dignity. 16

The European Union has indeed taken an approach to regulation with the proposed AI Act with its categorisation of certain types of artificial intelligence as high risk and mandatory

transparency obligations. The framework calls for disclosure where content is merely artificial and altered, resulting in informed consent and less deception.17

China has introduced certain regulations on synthetic media requiring any media created with AI to be clearly labelled as such, and making obligations on the service providers to avoid misuse. These rules represent one of the most singular approach to deepfake governance by statute and are emphasised by platform accountability and traceability.18

Comparatively, India has no specific legislation dealing with synthetic media and is instead based on general cyber and criminal laws which do not require proactive disclosure or labelling requirements.[2165]

9. Challenges in Regulation

One of the main concerns when handling deepfakes is the lack of ease for their detection. As AI models grow in sophistication, the synthetic content generated becomes more realistic and it becomes more difficult to distinguish from authentic media, thereby reducing the impact of forensic verification.2

Another challenge is the liar's dividend, in which the presence of deepfakes means that people can dismiss genuine audio-visual evidence as fake. This erodes confidence in digital media and makes the standards of proof difficult in court cases.2

Deepfakes also present jurisdictional challenges, where something can be produced in one place and live in another and is consumed everywhere. This makes enforcement difficult and creates conflicts of law with respect to which legal standards and remedies are applicable.

Platform liability is an ongoing hot debate. Intermediaries are provided safe harbour protections and are not ordinarily required to do anything except on notice. This reactive model is inadequate in light of the speed though which deepfakes disseminate as well as the irreparable damage they create.14

These challenges illustrate the fact that a complex of statutory reform, technological foreground detection measures, cross-border teamwork and a forward-minded intermediary obligation are necessary to introduce effective regulation.

10. Recommendations

The reality of the impact of this analysis shows the need for a dedicated Deepfake Regulation Act to be introduced in India which specifically recognises facial likeness, voice and other biometric attributes as attributes to be protected by law. Such legislation should define malicious synthetic media, prescribe civil and criminal liability for the creation and dissemination of malicious synthetic media and provide clear solutions to remedy victims such as injunctions, damages and takedown orders.15

A statutory requirement for mandatory watermarking and labelling of AI-generated content should be put in place so that there is transparency and people aren't deceived. Detection tools and tracking mechanisms at the platform-level would allow early detection of the synthetic media and minimise the risk of viral dissemination.16

The starting point for framing the legal framework should be the aim of adopting a consent based model of use of an individual's image and voice for a AI system. Any kind of commercial or public deployment of synthetic likeness without explicit authorisation should be considered a violation of personality and data protection rights. This is especially relevant for artists or famous people, for whom control over their identity is vital for their economic self-interest.

10. 2165 Digital Personal Data Protection Act, 2023; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
11. Shinu Vig, *Regulating Deepfakes: An Indian Perspective*, 17 J. STRATEGIC SECURITY 70 (2024). Vig-RegulatingDeepfakes-2024-1

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 1 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

There is also need for the criminalisation of the creation and distribution of malicious deepfakes, especially when the content is non-consensual explicit content, financial fraud, electoral manipulation and identity theft. Existing provisions on cheating and obscenity are not adequate to deal with the technological sophistication and scale of such offences.12

Finally, establishment of specialised fast-track cyber cells with technical expertise is needed for timely investigation, digital forensics and for coordinating takedown of harmful content. Given the pace that deepfakes spread, it is often the case that the delayed legal remedies can be ineffective.

11. Conclusion

Deepfakes and voice cloning are an especially revolutionary problem for the legal systems of our century by providing for the realistic manipulation of identity, and facilitating the rapid diffusion of false audio-visual content. The Indian legal framework is addressing these harm at currently is a patchwork of provisions relating to impersonation, defamation, obscenity and data protection. However, these laws were not meant to regulate biometric replication based on AI and they largely work in a reactive way.

The lack of statutory recognition of facial likeness and voice as protected attributes leaves large margins of protection of privacy, personality and economy without statutory protection. Victims have problems getting timely remedies and there are few proactive obligations for the platforms. The case studies discussed demonstrate that the deepfakes can lead to a loss of reputations, economic loss and psychological damage in a short time frame, often before effective legal intervention.

Comparative regulatory approaches, including for transparency obligations, labelling requirements and accountability for platforms, show that such transparencies are key components of an effective governance approach. India needs to put in place a future vision regulatory model that has criminal sanctions for mal use, civil remedies to the victim and technological safeguards like watermark and traceability.

At the same time, innovation should be balanced with fundamental rights through regulation. Deepfake technology has some legitimate use in education and accessibility and creative industries; a framework that is overly restrictive may abet technological development. The [2166]objective should therefore be to avoid harmful and deceptive uses and allow for lawful and consensual deployment.

A comprehensive legal framework that is fully AI-specific and that recognises biometric identity as a protected legal interest is urgently needed to protect dignity, reputation and democratic integrity in the digital age.15

12. Bibliography (ILI Style)

Articles

Shinu Vig, *Regulating Deepfakes: An Indian Perspective*, 17 J. STRATEGIC SECURITY 70 (2024).
Todd C. Helmus, *Artificial Intelligence, Deepfakes, and Disinformation: A Primer* (RAND Corporation, 2022).
Jon Bateman, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios* (Carnegie Endowment for International Peace, 2020).

Statutes

Information Technology Act, 2000.
Indian Penal Code, 1860.
Digital Personal Data Protection Act, 2023.
Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Case Law

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

12. 2166 Todd C. Helmus, *Artificial Intelligence, Deepfakes, and Disinformation: A Primer* (RAND Corporation, 2022). HELMUS-ArtificialIntelligenceDe…
13. Id.
14. Id.