The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

AI-GENERATED DEEPFAKES, PERSONALITY RIGHTS AND LAW

Are Existing Indian Legal Protections Sufficient to Protect Identity in the Age of Generative AI?

~ Bhumi Pal

INTRODUCTION

In September 2023, the Delhi High Court restrained a group of websites from exploiting actor Anil Kapoor's name, likeness, voice and signature expression without his consent, including through AI-based tools and face morphing.[1] Within a year, the Bombay High Court granted comparable relief to singer Arijit Singh against platforms offering to clone his voice.[2] Both orders point to the same problem: generative AI can now reproduce a person's face, voice and mannerisms so convincingly that an audience may believe the person actually appeared, spoke or endorsed something.

A deepfake is legally different from ordinary false content. The wrong does not lie only in what is said about a person; the person's own identity is used as raw material. This sets several values against each other: technological innovation, freedom of speech and an individual's control over her own persona. This article asks whether existing Indian legal protections are sufficient to protect personality rights against AI-generated deepfakes. It argues that Indian courts have built a workable but fragmented framework, and that deepfakes expose gaps in statutory clarity, enforcement and the protection of digital replicas, particularly for people who are not celebrities.

WHAT IS A DEEPFAKE?

A deepfake is synthetic media, created or altered with machine-learning models, that shows a real person saying or doing something they never said or did. India's 2026 amendments to the intermediary rules use the wider label ‘synthetically generated information’, covering audio,

[1] Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914 (Del. H.C.) (India).
[2] Arijit Singh v. Codible Ventures LLP, 2024 SCC OnLine Bom 2445 (Bom. H.C.) (India).

visual and audio-visual content created or altered by a computer resource so that it appears real.[3]

Four techniques matter for the law. Face-swapping places one person's face on another's body in a video. Voice cloning reproduces a person's speech from a short audio sample. Fully generated images and videos build a realistic scene from a text prompt. Synthetic audio can combine a cloned voice with scripted speech to fabricate calls, songs or endorsements. Between them, they can copy facial appearance, voice, body, expressions and speech patterns.

What makes this legally distinctive is that the content may be entirely fabricated while the person remains recognisable and is personally or commercially exploited. The legal concern therefore extends beyond whether the content is false; it concerns whether a person has control over the unauthorised digital use of their identity.

PERSONALITY RIGHTS, PRIVACY AND PUBLICITY RIGHTS DISTINGUISHED

Personality rights protect the identifiable aspects of a person's persona: name, image, likeness, voice, signature and other distinctive traits such as catchphrases or mannerisms. They are often confused with two neighbouring concepts, which are best kept apart.

Right	Core concern	Example
Privacy	Protection from unwanted intrusion into personal life	A fabricated intimate video of a private individual
Personality rights	Protection of personal identity and persona	A cloned voice or morphed face used without consent
Publicity rights	Control over commercial exploitation of identity	A fake celebrity endorsement of a product

These concepts overlap but are not identical. A fake endorsement video of a film star engages publicity (commercial value) and personality (identity); a fabricated intimate video of a private individual engages privacy and personality but has no commercial dimension at all.

The constitutional anchor is Article 21. In *Puttaswamy*, the Supreme Court recognised privacy as a fundamental right, including informational privacy and autonomy over personal identity.[4] Earlier, *R. Rajagopal* had linked privacy to a person's control over the publication of details of her life.[5] Yet the Constitution does not expressly create a standalone right of

[3] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India) (in force Feb. 20, 2026).
[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

personality. Indian protection has instead developed through privacy, passing off, publicity and common-law principles, largely in interim-injunction proceedings before the High Courts. That is why it is judge-made, celebrity-centred and uneven.

JUDICIAL DEVELOPMENT OF PERSONALITY RIGHTS IN INDIA

1. THE PASSING-OFF ERA

Indian courts first protected celebrity identity through passing off. In *D.M. Entertainment v. Baby Gift House*, the Delhi High Court restrained the sale of dolls modelled on singer Daler Mehndi and traded on his name and persona, treating his identity as commercially valuable and its misappropriation as actionable.[6] In *ICC Development v. Arvee Enterprises* (2003), the same court explained that the right of publicity is tied to an individual's identity, but held that it cannot be claimed by an event such as a cricket tournament; it belongs to an identifiable person.[7]

Titan Industries v. Ramkumar Jewellers (2012) concerned a jeweller that used photographs of Amitabh and Jaya Bachchan in its advertising without their consent. Relief went to a company that had engaged the couple as endorsers, and the court accepted that unauthorised commercial use of a celebrity's identity violates the right of publicity.[8] In *Shivaji Rao Gaikwad v. Varsha Productions* (2015), the Madras High Court restrained a film titled after actor Rajinikanth, holding that an identifiable celebrity need not prove confusion or falsity to protect his persona; identification is enough.[9] The Supreme Court's decision in *Puttaswamy* (2017) then supplied the constitutional foundation discussed above.[10]

2. THE DIGITAL EXPLOITATION PHASE

The most recent phase involves digital exploitation. In *Amitabh Bachchan v. Rajat Nagi* (2022), the Delhi High Court granted an interim injunction against unauthorised commercial use of the actor's name, voice, image and likeness across digital and other media.[11] *Anil Kapoor* (2023) is the direct bridge to deepfakes: the court protected his name, likeness, voice and catchphrase, and its order expressly contemplated AI tools and morphing as modes of misuse.[12] In *Arijit Singh* (2024), the Bombay High Court extended protection to a singer's

[5] R. Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632 (India).
[6] D.M. Entertainment Pvt. Ltd. v. Baby Gift House, 2010 (42) PTC 620 (Del.) (India).
[7] ICC Dev. (Int'l) Ltd. v. Arvee Enters., 2003 (26) PTC 245 (Del.) (India).
[8] Titan Indus. Ltd. v. Ramkumar Jewellers, 2012 (50) PTC 486 (Del.) (India).
[9] Shivaji Rao Gaikwad v. Varsha Prods., 2015 (62) PTC 351 (Mad.) (India).
[10] Puttaswamy, (2017) 10 S.C.C. 1.
[11] Amitabh Bachchan v. Rajat Nagi, 2022 SCC OnLine Del 4110 (Del. H.C.) (India).
[12] Anil Kapoor, 2023 SCC OnLine Del 6914.

voice against AI voice-cloning services, drawing on both personality rights and performer's rights.[13]

A pattern emerges. Relief is mostly interim, it is granted to well-known persons, and it rests on identifiability and commercial value rather than on any statute. That is a strong base, but a thin one.

STATUTORY FRAMEWORK

1. INFORMATION TECHNOLOGY ACT, 2000

Section 66C punishes the fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature, and section 66D punishes cheating by personation using a computer resource.[14] Both were drafted with credential theft and online fraud in mind. A deepfake used to cheat may fit section 66D, but a non-deceptive clone, or one made to harass, may not. Section 66E is framed around images of a private area captured without consent, which fits synthetic images awkwardly, while sections 67 and 67A treat sexually explicit deepfakes as obscenity rather than as a violation of the victim's consent.[15]

2. INTERMEDIARY RULES

Safe harbour for platforms under section 79 depends on due diligence, and *Shreya Singhal* confined takedown duties to cases of actual knowledge, meaning a court or government order.[16] The 2021 Rules added a duty to act on complaints about impersonation, including artificially morphed images, within 24 hours,[17] and the Ministry of Electronics and Information Technology issued a deepfake advisory in December 2023.[18] The 2026 Amendment Rules, in force since 20 February 2026, go further: they define synthetically generated information, require prominent labelling and provenance metadata, and shorten takedown timelines for unlawful content, in some cases to three hours.[19] The question is whether obligations placed on intermediaries can protect a person against an anonymous creator who is never a party to the proceeding.

---

[13] Arijit Singh, 2024 SCC OnLine Bom 2445.
[14] Information Technology Act, 2000, No. 21 of 2000, §§ 66C, 66D (India).
[15] Information Technology Act, 2000, No. 21 of 2000, §§ 66E, 67, 67A (India).
[16] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India); Information Technology Act, 2000, No. 21 of 2000, § 79 (India).
[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), r. 3(2)(b) (Feb. 25, 2021) (India).
[18] Ministry of Electronics & Information Technology, Advisory on Due Diligence by Intermediaries Under the IT Rules (Dec. 26, 2023) (India).
[19] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India).

3. DIGITAL PERSONAL DATA PROTECTION ACT, 2023

A face or voice that identifies a person is personal data, so building a deepfake from it generally needs consent or a listed lawful ground.[20] But the Act does not apply to personal data that the individual herself has made publicly available, a carve-out that may weaken protection where photographs and clips are scraped from social media.[21] It is also a data-protection statute enforced through a regulator, not an injunction-and-damages remedy for the individual. It is relevant to deepfakes, but it is not a deepfake law.

4. COPYRIGHT

A face or voice is not itself a copyrightable work. Copyright protects original works, while personality rights protect identity. A deepfake may infringe copyright if it reproduces a particular film, photograph or recording, but a wholly synthetic likeness may copy no protected work at all. Performer's rights help performers, as *Arijit Singh* shows, but they do not help everyone else.[22]

5. TRADEMARK AND PASSING OFF

Section 27(2) of the Trade Marks Act preserves passing-off remedies, the courts' original vehicle for celebrity claims.[23] This route works where there is deception, false association or commercial misappropriation, but fits poorly where a deepfake is non-commercial.

6. NO DEDICATED FRAMEWORK

India has several laws that may apply to a deepfake but no single statute that governs it. The 2026 Rules regulate platforms and labelling; they do not create a right for the person depicted.

7. CHOOSING THE ROUTE

One deepfake may simultaneously involve privacy, personality rights, defamation, copyright, data protection and intermediary liability. A victim must decide which route to take, in which forum, often within hours.

GAPS AND GREY AREAS

1. CONSENT AND NON-COMMERCIAL REPLICAS

[20] Digital Personal Data Protection Act, 2023, No. 22 of 2023, §§ 2(t), 4, 7 (India).
[21] Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 3(c)(ii) (India).
[22] Copyright Act, 1957, No. 14 of 1957, §§ 38, 38B (India).
[23] Trade Marks Act, 1999, No. 47 of 1999, § 27(2) (India).

What if a person's face is replicated, their voice cloned and their identity placed in a fictional scenario, but nothing is sold? Personality rights are not limited to advertisements, and recent orders have protected identity beyond commerce, but this rests on interim orders rather than settled law.

2. CELEBRITIES AND ORDINARY PEOPLE

Nearly all reported orders concern well-known persons whose identity has commercial value. Yet the most serious harms, such as non-consensual sexual deepfakes or cloned voices used in fraud, commonly fall on ordinary people who cannot easily afford a High Court suit. Personality-rights jurisprudence should become more accessible beyond celebrities.

3. ENFORCEMENT ACROSS BORDERS

The creator may be anonymous, outside India, on a foreign platform or operating through many accounts. Intermediary rules bind platforms that operate in India, but they do not reach every source of the content.

FREE SPEECH AND THE LIMITS OF REGULATION

Should every AI-generated representation of a person be prohibited? Plainly not. Article 19(1)(a) protects speech, and restrictions must fall within the grounds in Article 19(2).[24] Parody, satire, criticism, political commentary, journalism, documentaries and fiction all routinely use a real person's identity, and *Rajagopal* recognised that publication drawn from matters of public record does not violate privacy.[25]

The workable line is between legitimate expression on one side and commercial exploitation, deception and harmful impersonation on the other. A clearly labelled parody of a politician is unlikely to deceive; a cloned voice used to solicit money almost certainly does. Labelling therefore supports both interests, though civil-society groups have warned that compressed takedown windows and mandatory labelling can push platforms towards over-removal.[26] The law does not need an absolute position on synthetic media; it needs criteria that separate expression from exploitation.

REMEDIES AVAILABLE TODAY

1. CIVIL REMEDIES

[24] India Const. art. 19(1)(a), 19(2).
[25] Rajagopal, (1994) 6 S.C.C. 632.
[26] Internet Freedom Found., IT Intermediary Amendment Rules, 2026 Contradict Their Purpose (Feb. 12, 2026), https://internetfreedom.in/it-intermediary-amendment-rules-2026-contradict-their-purpose/.

The principal remedy is an injunction, often an interim or ex parte order that also binds unnamed defendants, together with damages, delivery-up of infringing material and takedown directions. Claims may be framed as personality or publicity rights, passing off or privacy.

2. CRIMINAL REMEDIES

Depending on the facts, prosecution may proceed for cheating by personation, defamation, identity theft or transmission of sexually explicit material.[27]

3. PLATFORM REMEDIES

Victims can report content to the platform's grievance mechanism and invoke the intermediary's duties under the rules.[28]

The practical difficulty is speed. Getting content removed quickly is often more important than obtaining damages years later, because a deepfake can spread widely within hours. Shorter takedown windows help, but they still depend on the victim knowing where to complain and on the platform acting.

THE WAY FORWARD: REFORM PROPOSALS

1. STATUTORY RECOGNITION

India could consider expressly recognising a person's name, image, likeness, voice and digital replica as protected interests, so that protection does not depend on interim orders and celebrity status.

2. GRADED REGULATION OF AI IMPERSONATION

The law should distinguish harmless synthetic content, parody and satire, commercial exploitation, deceptive impersonation, sexually explicit deepfakes and political or electoral deepfakes, and attach different consequences to each.

3. FASTER, MORE ACCESSIBLE TAKEDOWN

Where identity is clearly identifiable, consent is absent and the content is harmful or deceptive, a rapid complaint route should exist for ordinary individuals, not only for those who can litigate.

4. TRANSPARENCY AND PROVENANCE

---

[27] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 319, 356 (India); Information Technology Act, 2000, No. 21 of 2000, §§ 66C, 66D, 67A (India).

[28] See Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India).

Labelling, provenance metadata and watermarking are now part of the 2026 Rules, so the reform question is less whether to require them than whether they work, given the unreliability of detection tools and the ease of stripping metadata.

5. PROTECTION BEYOND CELEBRITIES

A statutory remedy with simple procedure and available relief for non-commercial harm would bring ordinary victims within the framework that celebrities have already secured.

CONCLUSION

AI-generated deepfakes expose a gap between the speed of technological development and the evolution of personality-rights law. Indian courts have progressively recognised protection over an individual's identity, from *D.M. Entertainment* to *Anil Kapoor* and *Arijit Singh*, but that protection has developed through fragmented doctrines and interim orders rather than a comprehensive statute. The 2026 amendments to the intermediary rules add labelling and faster takedown, yet they regulate platforms rather than confer rights on the person depicted.

The answer to the central question is therefore qualified. Existing law protects several aspects of identity, especially for public figures, but it is not yet sufficient for voice cloning, synthetic video and digital replicas, or for ordinary victims. Reform should clarify the rights, target deception and harmful impersonation, and preserve space for satire, criticism and artistic expression.