

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

FACES, VOICES AND FABRICATIONS: DEEPFAKES, IDENTITY MANIPULATION AND THE PROTECTION OF PERSONALITY RIGHTS IN THE DIGITAL AGE

AUTHORED BY - AKSHAT MEHTA

Ph.D. Scholar, Hidayatullah National Law University

Abstract

Synthetic media, popularly called "deepfakes", allow anyone with a consumer device to fabricate a convincing image, video or voice of a real person saying or doing things that never happened. This paper examines deepfakes as a technology of identity manipulation and asks whether existing personality-rights law can answer the harm they cause. The paper explains the nature, evolution and technical architecture of deepfakes, the ecosystem that produces them, the harms they generate and the limits of detection. It analyses the legal challenges, with principal reference to India: the constitutional foundations of personality and privacy rights, the judge-made protection of celebrity personas, statutory remedies under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Copyright Act, 1957 (especially performers' rights) and the Digital Personal Data Protection Act, 2023, and the 2026 amendment to the IT Rules on synthetically generated information. Comparative developments in the United States, the European Union, China and Denmark are used as benchmarks. The paper argues that Indian courts have been inventive but that the protection remains fragmented, injunction-centred and dependent on platform cooperation, and it proposes a consent-based, technology-neutral statutory framework for digital replicas.

Keywords: deepfakes; synthetic media; personality rights; right of publicity; voice cloning; digital replicas; intermediary liability; performers' rights.

1. Introduction

For most of legal history, a person's identity was protected against misuse of a *copy*: a photograph taken without consent, a name used on a product, an impersonator on a stage. The copy was recognisably a copy. Deepfakes change the problem in kind. The output is not a reproduction of something that existed but a fresh fabrication that is statistically indistinguishable from reality, generated at scale and near-zero cost. The person depicted has

not been copied; they have been *conjured*.¹

This matters for three reasons. First, the harm is intimate: it attaches to face, voice, body and reputation, the core of what personality rights are meant to protect. Second, the harm is systemic: when any recording can be fabricated, genuine recordings lose evidentiary value, a danger Chesney and Citron called the "liar's dividend". Third, the law's traditional tools (defamation, passing off, copyright, privacy) each capture only a slice of the wrong.

This paper first examines the nature, technologies and social consequences of deepfakes, and then analyses the legal challenges they pose to personality rights, with particular attention to India and comparative approaches. It concludes with recommendations for a coherent and rights-sensitive framework.

2. Nature and Technology of Deepfakes

2.1 Concept and Origins

"Deepfake" is a portmanteau of *deep learning* and *fake*. The word entered public use in late 2017, when a Reddit user with that handle posted face-swapped explicit videos made with open-source neural-network tools. Within months, easy-to-use applications had spread the technique far beyond specialists.²

In technical terms, a deepfake is synthetic or manipulated audio, visual or audio-visual content, produced or altered by machine-learning models, that depicts a real person (or a realistic but non-existent one) in a way that appears authentic. Three features distinguish it from older forms of manipulation such as photo-editing or film trickery:

- **Automation:** the model learns the target's features from data; no frame-by-frame manual craft is needed.
- **Realism:** outputs can defeat casual human inspection, including of motion, lighting and speech.
- **Scalability:** once a model is trained, producing thousands of variants costs almost nothing.

It is useful to separate *deepfakes* from *cheapfakes* (crude edits such as slowed-down video or misleading captions) and from *wholly synthetic personas* (generated faces with no real-world counterpart). The legal analysis differs: identity manipulation in the strict sense arises where a **real, identifiable person** is depicted.

1 Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107 California Law Review 1753.

2 Ibid; see also Deepttrace, The State of Deepfakes: Landscape, Threats, and Impact (2019).

2.2 Core Technologies

- (a) **Autoencoders and face swapping.** The first wave of deepfakes used paired autoencoders. A shared encoder compresses faces into a compact representation of expression and pose; separate decoders reconstruct the faces of two different people. Swapping decoders at run time renders person A's face with person B's expressions.
- (b) **Generative Adversarial Networks (GANs).** Introduced by Goodfellow and colleagues in 2014, GANs pit a *generator* that fabricates images against a *discriminator* that tries to tell them from real ones. Training continues until the discriminator is fooled. GAN variants such as StyleGAN made photo-realistic faces routine.³
- (c) **Diffusion models.** More recent systems (following Ho, Jain and Abbeel, 2020, and latent-diffusion work by Rombach and others, 2022) generate images and video by learning to reverse a gradual noising process. They produce higher fidelity and finer control through text prompts, and now underpin much text-to-image and text-to-video generation.⁴
- (d) **Face reenactment and lip-sync.** Rather than swapping a face, these methods transfer the expressions or head movements of a driving performer onto a target, or adjust the target's mouth to match new audio. This allows a real video to be given a new script.
- (e) **Voice cloning and speech synthesis.** Neural text-to-speech and codec-based language models can reproduce a speaker's timbre, accent and cadence from a short sample, in some systems a matter of seconds. Voice deepfakes are particularly dangerous because audio is cheap to transmit, hard to scrutinise and routinely trusted in phone-based fraud.
- (f) **Real-time and multimodal pipelines.** Live face-swapping on video calls and integrated systems that generate synchronised video and speech have moved deepfakes from pre-produced clips to interactive impersonation.

2.3 The Production Ecosystem

The technical barrier has collapsed. Open-source repositories, mobile applications, "nudify" bots and subscription cloning services allow non-experts to create deepfakes in minutes. Training material is typically scraped from public social-media profiles, interviews and film or television footage, a fact with direct consequences for consent, data-protection and copyright analysis (discussed below). Distribution is through social-media platforms, messaging

3 Ian Goodfellow et al., "Generative Adversarial Nets" (2014) *Advances in Neural Information Processing Systems* 27.

4 Jonathan Ho, Ajay Jain and Pieter Abbeel, "Denoising Diffusion Probabilistic Models" (2020); Robin Rombach et al., "High-Resolution Image Synthesis with Latent Diffusion Models" (2022).

applications and adult-content sites, where virality outpaces moderation.

2.4 Typology of Identity-Manipulation Harms

Category	Illustration	Principal interest harmed
Non-consensual intimate imagery	Face of a woman grafted onto explicit video	Dignity, bodily autonomy, reputation
Fraud and impersonation	Cloned voice of a relative or executive requesting a transfer; fake celebrity endorsements	Property, consumer trust, identity
Political and electoral manipulation	Fabricated speech by a candidate before polling	Democratic integrity, reputation
Commercial exploitation	Using a performer's likeness or voice in advertising or AI-generated songs without licence	Economic value of persona
Harassment and extortion	Fake compromising content used for blackmail or bullying	Safety, mental integrity
Evidentiary erosion	Genuine footage dismissed as "fake"	Truth-finding, accountability

Empirical studies have consistently found that the bulk of deepfake content online is sexual and overwhelmingly targets women. A widely cited 2019 report by Deepttrace (now Sensity) found that about 96 per cent of deepfake videos then identified were non-consensual pornography. Whatever the exact current proportion, the pattern shows that deepfakes are not merely a speech or misinformation problem; they are a gendered form of image-based abuse.⁵

2.5 Detection, Provenance and the Limits of Technology

Technical responses fall into two families.

Detection looks for traces of synthesis: visual artefacts, inconsistent lighting or reflections, unnatural blinking or head motion, spectral fingerprints of generators, audio-visual mismatches and physiological signals such as subtle colour changes caused by blood flow. Detection faces structural problems. It is an arms race, since each published detector can be used to train a better generator. Detectors often generalise poorly to new generation methods, degrade under compression and re-uploading, and generate false positives that can themselves damage

⁵ Deepttrace, *The State of Deepfakes: Landscape, Threats, and Impact* (2019) (reporting that approximately 96 per cent of deepfake videos identified in its study were non-consensual pornography).

genuine speakers.

Provenance inverts the question: instead of proving content is fake, it proves where authentic content came from. Methods include cryptographic content credentials (such as the C2PA standard), invisible watermarks embedded by generators, and platform-level labelling. Provenance works only if adopted widely, survives editing and re-encoding, and is not stripped by bad actors; malicious tools outside the standard ecosystem will simply omit it.

The lesson for lawyers is that technology alone cannot settle authenticity. Law must therefore allocate responsibility among creators, tool providers and platforms, and must fix evidentiary rules for a world in which "seeing is believing" no longer holds.

2.6 Beneficial and Neutral Uses

Deepfake technology is not inherently unlawful. It supports film dubbing and de-ageing, accessibility tools that restore a voice to patients, education and museum experiences, satire and parody, and privacy-protective anonymisation. Any legal response must therefore be calibrated to *non-consensual, deceptive or harmful use* rather than to the technique itself, so that expression and legitimate innovation are not suppressed.

3. Legal Challenges and Responses under Personality Rights

3.1 Meaning and Scope of Personality Rights

Personality rights protect an individual's control over the use of attributes that identify them, such as name, image, likeness, voice, signature, mannerisms and distinctive catchphrases. They have two overlapping strands:

1. a **dignitary or privacy strand**, protecting against intrusion, humiliation and false portrayal; and
2. a **proprietary or publicity strand**, protecting the commercial value in a persona against unauthorised exploitation.

Common-law systems arrived at these ideas through different routes: the US right of publicity (from *Haelan Laboratories v. Topps Chewing Gum*, 1953, and Nimmer's 1954 article), the privacy torts catalogued by Prosser in 1960, and, in India, a mosaic of constitutional privacy, passing off and statute. Civil-law systems generally treat personality as a protected personal interest in their civil codes and data-protection law.⁶

⁶ *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1953); Melville B. Nimmer, "The Right of Publicity" (1954) 19 *Law and Contemporary Problems* 203; William L. Prosser, "Privacy" (1960) 48 *California Law Review* 383.

3.2 Technological Challenges to Traditional Doctrine

Deepfakes expose several points where doctrine built for a pre-synthetic world strains.

1. **Fabrication, not copying.** Copyright and passing off assume an existing work or goodwill that has been reproduced or traded on. A synthetic video reproduces no particular frame; it is novel content. Defamation requires a false statement that lowers reputation, but a flattering deepfake, or one that falls short of defamatory meaning, may still violate dignity or autonomy.
2. **Anonymity and cross-border reach.** Creators are frequently pseudonymous, use VPNs and host content abroad, making identification, service of process and enforcement difficult.
3. **Speed and scale.** Harm is done within hours of upload; litigation takes months. Content is re-posted and re-encoded endlessly, so takedown of one copy rarely ends the harm.
4. **Distributed responsibility.** A deepfake involves a dataset curator, a model developer, a tool operator, the person who prompts, a platform and downstream sharers. Traditional doctrines assume a single wrongdoer.
5. **Consent is hard to locate.** Training data is scraped from public posts; whether publicly available data may be repurposed to clone a person is contested.
6. **Proof and evidence.** Courts must now authenticate audio-visual evidence, and genuine evidence can be disputed as fabricated.
7. **Speech trade-offs.** Satire, parody, political commentary and artistic work often use a person's likeness, so broad prohibitions risk chilling protected expression.

3.3 Constitutional Foundations in India

India has no single statute on personality rights; courts have derived them from constitutional and common-law principles.

Privacy and dignity. In *R. Rajagopal v. State of Tamil Nadu* ((1994) 6 SCC 632), the Supreme Court recognised the right to privacy as implicit in Article 21 and held that a person has a right to control the publication of matters concerning their private life, with exceptions for public records and, within limits, public figures. In *Justice K.S. Puttaswamy v. Union of India* ((2017) 10 SCC 1), a nine-judge Bench held privacy to be a fundamental right and recognised informational privacy, autonomy and dignity as its components. A deepfake of a person's body or voice engages precisely these interests: control over self-presentation and over data about

the self.⁷

Freedom of expression. Article 19(1)(a) protects parody, satire and criticism, and Article 19(2) allows only enumerated, reasonable restrictions. Any statutory or judicial limit on deepfakes must therefore be justified under defamation, decency, public order or similar heads and must be proportionate. This tension is the legitimate core of the counter-argument to over-broad regulation.⁸

3.4 Judicial Development of Personality Rights in India

Indian courts, especially the Delhi and Bombay High Courts, have built a body of personality-rights jurisprudence largely through interim injunctions in suits for passing off and violation of privacy and publicity.

- *ICC Development (International) Ltd v. Arvee Enterprises* (Delhi High Court, 2003) recognised that a person's right of publicity flows from the right of privacy and that the right to commercial value in identity belongs to the individual.⁹
- *Titan Industries Ltd v. Ramkumar Jewellers* (Delhi High Court, 2012) protected the images of Amitabh and Jaya Bachchan against unauthorised use in advertising, emphasising identifiability and commercial misappropriation.¹⁰
- *D.M. Entertainment v. Baby Gift House* (Delhi High Court, 2010) protected the singer Daler Mehndi's persona against sale of look-alike dolls, and *Shivaji Rao Gaekwad v. Varsha Productions* (Madras High Court, 2015) addressed use of the actor's identity in a film title, illustrating the limits of the doctrine where the person is not identified.¹¹
- *Amitabh Bachchan v. Rajat Nagi* (Delhi High Court, 2022) restrained misuse of the actor's name, voice and image in fraudulent schemes.

The jurisprudence entered the synthetic-media era in *Anil Kapoor v. Simply Life India* (Delhi High Court, 2023), where the court granted wide interim protection over the actor's name, image, voice, likeness and signature catchphrase, expressly restraining misuse through artificial intelligence, face morphing and similar technology, and extending relief against unidentified defendants. In *Jackie Shroff v. The Peppy Store* (Delhi High Court, 2024), the court protected the actor's name and manner of speech, including against AI-driven chatbots. In *Arijit Singh v.*

7 R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

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

9 ICC Development (International) Ltd v. Arvee Enterprises, 2003 (Delhi High Court).

10 Titan Industries Ltd v. Ramkumar Jewellers, 2012 (Delhi High Court).

11 D.M. Entertainment Pvt. Ltd v. Baby Gift House, 2010 (Delhi High Court); Shivaji Rao Gaekwad v. Varsha Productions, 2015 (Madras High Court).

Codible Ventures LLP (Bombay High Court, 2024), the court restrained AI voice-cloning applications that imitated a singer's voice, and treated a performer's attributes as protectable. Through 2025, the Delhi and Bombay High Courts passed a stream of similar orders for prominent film and public personalities, many of them directed at deepfakes, AI-generated content and unlicensed merchandise.¹²

Three features of this case law deserve emphasis:

1. **Expansion of protected attributes**, from name and photograph to voice, mannerisms, catchphrases and AI-generated likeness.
2. **Remedial innovation**, including "John Doe" (*Ashok Kumar*) orders against unknown defendants, directions to platforms to take down and disclose subscriber data, and dynamic-style injunctions that cover mirror content.
3. **Celebrity bias**. Most reported relief goes to well-known persons who can fund High Court litigation and show commercial reputation. The ordinary woman whose face appears in a fabricated explicit video has no comparable access to a personality-rights suit, and must rely on criminal complaints and platform grievance systems.

3.5 Statutory Responses in India

India's statutes reach deepfakes indirectly. The principal provisions are mapped below.¹³

Instrument	Relevant provisions	Limitation
Information Technology Act, 2000	s. 66C (identity theft), s. 66D (cheating by personation using a computer resource), s. 66E (violation of privacy), ss. 67, 67A, 67B (obscene, sexually explicit and child-abuse material), s. 69A (blocking), s. 79 (intermediary safe harbour)	Drafted before synthetic media; "identity theft" is tied to fraudulent use of passwords and unique identifiers; no express deepfake offence
Bharatiya Nyaya Sanhita, 2023	Defamation (s. 356), cheating by personation (s. 319), forgery to harm reputation (s. 336), stalking and voyeurism (ss. 77 and 78), insulting the modesty of a woman (s. 79), obscenity (s. 294)	Offence-by-offence fit; deepfakes require stretching definitions of "forgery" and "false document"

12 Anil Kapoor v. Simply Life India, 2023 (Delhi High Court); Jackie Shroff v. The Peppy Store, 2024 (Delhi High Court); Arijit Singh v. Codible Ventures LLP, 2024 (Bombay High Court).
13 Information Technology Act, 2000, ss. 66C, 66D, 66E, 67, 67A, 67B, 69A and 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended.

Instrument	Relevant provisions	Limitation
Copyright Act, 1957	s. 14 (exclusive rights), s. 38 (performers' rights), s. 38B (performers' moral rights), s. 57 (author's special rights), s. 52(1)(a) (fair dealing)	Protects works and performances, not a person's likeness as such
Digital Personal Data Protection Act, 2023	Notice and consent for processing digital personal data; rights of correction and erasure; duties of data fiduciaries	Exemptions for personal or domestic use and for data made publicly available; no explicit synthetic-media provisions
Trade Marks Act, 1999 and passing off	s. 2(1)(m) (a "mark" includes a name or signature); ss. 29 and 30	Requires trade use and goodwill; weak for private individuals

(a) Information Technology Act and Rules. Sections 66C and 66D are the usual prosecutorial tools against impersonation, and s. 66E addresses capture and transmission of private images. Section 67A and 67B cover sexually explicit and child-abuse material, which includes synthetic versions where the content depicts such acts. Section 69A allows blocking on specified grounds. Under s. 79, intermediaries are exempt from liability for third-party content if they observe due diligence; in *Shreya Singhal v. Union of India* ((2015) 5 SCC 1), the Supreme Court read down the knowledge requirement in s. 79(3)(b) to actual knowledge acquired through a court order or government notification. The 2021 Intermediary Guidelines and Digital Media Ethics Code Rules added due-diligence duties, including a duty to remove content that exposes a person's private area or depicts impersonation in electronic form, on complaint.¹⁴

(b) The 2026 amendment on synthetically generated information. The Ministry of Electronics and Information Technology notified an amendment to the IT Rules on 10 February 2026, effective from 20 February 2026, which for the first time expressly brings "synthetically generated information" (SGI) within the intermediary due-diligence framework. SGI is defined as audio, visual or audio-visual information that is artificially or algorithmically created or altered in a way that appears real and is likely

¹⁴ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

to be perceived as indistinguishable from a real person or event. Reported features of the amendment include:¹⁵

- mandatory, prominent labelling of SGI, with embedded metadata or unique identifiers, and a bar on removing or suppressing labels;
- additional obligations on significant social media intermediaries, including seeking user declarations on whether content is synthetic and verifying them with technical measures before publication;¹⁶
- prohibition on certain categories of SGI, such as child sexual abuse material, non-consensual intimate imagery, false documents and deceptive impersonation;¹⁷
- sharply compressed timelines, including disabling access within three hours of a lawful order and shorter grievance-redressal periods; and¹⁸
- a clarification that good-faith removal of such content in accordance with the rules does not forfeit safe harbour, while non-compliance may.

This is a significant structural step: it moves India from case-by-case injunctions toward a systemic, platform-facing regime. Its limits are also evident. It regulates intermediaries rather than creating a personal right of action for the depicted individual; it addresses audio and visual content but not text; it depends on detection and declaration systems that are imperfect; and it is vulnerable to constitutional challenge on proportionality and over-removal grounds, particularly with very short takedown windows. Readers should consult the notified text for the exact rule numbers and compliance thresholds.¹⁹

(c) Copyright and related rights. An important connection is performers' rights. Section 38 gives performers exclusive rights over their performances, and s. 38B gives performers moral rights to claim identification and to restrain distortion, mutilation or modification prejudicial to their reputation. A deepfake that re-uses a recorded performance with altered speech or expression can engage these provisions, and s. 57

15 Ministry of Electronics and Information Technology, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, notified 10 February 2026, effective 20 February 2026 (as described in the source paper; consult the notified text for exact rule numbers and thresholds).

16 Copyright Act, 1957, ss. 14, 38, 38B, 52(1)(a) and 57.

17 Digital Personal Data Protection Act, 2023. The precise application of its public-availability exclusion depends on the statutory text and circumstances of processing.

18 Bharatiya Nyaya Sanhita, 2023, including ss. 77, 78, 79, 294, 319, 336 and 356; Bharatiya Sakshya Adhiniyam, 2023.

19 California Civil Code § 3344; Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988); Waits v. Frito-Lay, Inc., 978 F.2d 1093 (9th Cir. 1992); TAKE IT DOWN Act (2025); Tennessee ELVIS Act (2024).

may assist authors where a work is distorted. The Bombay High Court's Arijit Singh order used such reasoning in treating a singer's vocal performance as protectable. The limits are significant. Copyright protects fixed works and recorded performances, not a face or voice in the abstract; a wholly synthetic voice that imitates style without reproducing any recording may fall outside; and the fair-dealing exceptions in s. 52(1)(a), which cover criticism and review, are narrower than the American doctrine of fair use. Training on copyrighted film or music raises separate reproduction-right questions about how far scraping is permitted in the absence of a text-and-data-mining exception.

- (d) Data protection.** A person's face and voice are personal data when they identify the person, so scraping and processing them to build a clone ordinarily needs a lawful basis. The DPDP Act, 2023 centres on notice and consent and provides correction and erasure rights, but excludes from its scope personal data that the individual themselves has made publicly available, which can weaken protection against scraping of public social-media content. Because the Act regulates the processing of data rather than the output, it does not itself say when a synthetic depiction is unlawful.²⁰
- (e) Criminal law.** The Bharatiya Nyaya Sanhita offers several routes (defamation, forgery to harm reputation, cheating by personation, offences against women), but none was drafted with synthetic media in mind. Prosecutors must fit deepfakes into definitions of "false document" or "false electronic record", and punishments vary widely. Investigation also depends on cross-border cooperation and platform data.

3.6 Comparative Perspectives

United States. There is no federal right of publicity; protection comes from state statutes and common law (for example California Civil Code s. 3344). Landmark cases include *Zacchini v. Scripps-Howard Broadcasting* (U.S. 1977), *Midler v. Ford Motor Co.* (9th Cir. 1988) and *Waits v. Frito-Lay* (9th Cir. 1992), which protected a distinctive voice imitated by sound-alike, and *White v. Samsung* (9th Cir. 1992). States have since legislated specifically: Tennessee's ELVIS Act (2024) expressly covers AI voice cloning, and many states have criminalised sexual deepfakes. At federal level, the TAKE IT DOWN Act (signed in May 2025) criminalises publication of non-consensual intimate imagery, including AI-generated imagery, and requires covered platforms to remove it on notice. Proposals such as the NO FAKES Act, which would

²⁰ Provisions on the Administration of Deep Synthesis of Internet Information Services (China, 2023); see also the source paper's discussion of Chinese AI-content labelling measures effective in 2025.

create a federal right in digital replicas, have been discussed but should be checked for current status.

European Union. The General Data Protection Regulation treats facial and voice data as personal data, and biometric data used for identification as a special category, giving rights of objection and erasure. The Digital Services Act imposes notice-and-action and systemic-risk duties on platforms. The AI Act (Regulation (EU) 2024/1689) imposes transparency obligations on those who deploy deepfakes, requiring disclosure that content is artificially generated or manipulated, with exceptions for evidently artistic or satirical works; the timetable for these provisions should be confirmed against current implementation measures.

China. The Provisions on the Administration of Deep Synthesis of Internet Information Services (in force from January 2023) require consent of the persons whose biometric information is edited, real-name verification and labelling, and national measures on labelling of AI-generated content took effect in September 2025.

Denmark. A widely discussed Danish proposal would amend copyright law to give individuals rights over their own body, face and voice, allowing removal demands against platforms and compensation. Its significance is conceptual: it treats likeness as something close to a protectable work, which is the very bridge between personality rights and related rights that this course explores.²¹

3.7 Critical Analysis: Gaps in the Indian Response

- 1. No statutory personality right.** Protection rests on judicial creativity, producing uncertainty about scope, duration, post-mortem rights, assignment and licensing.
- 2. Celebrity-centred access.** The remedy works best for those with commercial persona. Ordinary victims, especially women targeted with sexual deepfakes, need fast, low-cost relief.
- 3. Fragmented liability.** Offences and civil wrongs are scattered across statutes. Developers and distributors of deepfake tools are rarely addressed directly.²²
- 4. Platform dependence and over-removal risk.** The 2026 Rules place heavy duties on intermediaries. Very short takedown timelines may encourage automated over-blocking of lawful parody and political speech, without adequate appeal.

21 See Chesney and Citron (n 1); compare the platform and transparency obligations described in the Information Technology Rules, 2021, as amended in 2026.

22 Copyright Act, 1957, s. 38B; Bharatiya Sakshya Adhiniyam, 2023 (rules governing electronic records and their evidentiary treatment).

5. **Evidence and attribution.** Courts and police lack standard tools to authenticate synthetic media and trace anonymous creators.
6. **Weak treatment of consent and licensing.** Law rarely distinguishes licensed digital replicas (for example, an actor's authorised AI de-ageing) from unlicensed ones, so there is no clear market structure for lawful use.
7. **Freedom of expression.** There is no clear statutory carve-out for satire, news reporting, education and artistic works, which leaves courts to balance case by case.

3.8 Recommendations

1. **Enact a technology-neutral personality-rights statute** protecting name, image, voice, likeness and distinctive attributes of every natural person (not only celebrities), covering digital replicas, with defined exceptions for news, satire, parody, criticism and bona fide artistic or educational use.
2. **Create a consent and licensing framework for digital replicas:** written, specific, time-limited consent; restrictions on perpetual or blanket transfers; fair remuneration; and post-mortem rules. Performers' moral rights under s. 38B should be clarified to cover synthetic alteration.
3. **Address image-based abuse directly** through a specific offence of creating or sharing non-consensual intimate synthetic imagery, plus an emergency civil remedy and a victim-support mechanism including a single-point takedown route and hash-matching to prevent re-upload.
4. **Calibrate platform duties** with procedural safeguards: reasoned orders, counter-notice and review for lawful speech, transparency reports, and proportionate timelines distinguishing intimate-abuse content from other categories.
5. **Impose duties on the supply chain**, such as safeguards, watermarking and provenance standards for generative-AI providers, and restrictions on tools designed to produce non-consensual sexual imagery.
6. **Build institutional and evidentiary capacity:** forensic laboratories, judicial training, and rules of evidence on authentication of electronic records under the Bharatiya Sakshya Adhiniyam, 2023.
7. **Promote international cooperation and media literacy**, recognising that technology cannot be countered by law alone.

4. Conclusion

Deepfakes are a stress test for personality rights. Technologically, they combine generative models, abundant public data and low-cost tools to fabricate a person's face and voice with startling realism, while detection lags and provenance remains incomplete. Legally, India has responded in layers: constitutional recognition of privacy and dignity, a vigorous line of High Court injunctions protecting persona, scattered statutory offences, and, since February 2026, a platform-oriented regime for synthetically generated information. These developments are real progress, but they remain remedial, celebrity-weighted and dependent on intermediaries.

The next stage should shift from reacting to specific fakes toward a coherent right of control over one's digital self: consent-based, applicable to everyone, enforceable quickly and balanced against free expression. A framework of that kind would also connect personality rights with copyright's related rights, treating the performer's voice, face and performance as assets that can be licensed, but never conscripted.

