INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

ISSN: 2582-6433

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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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.

ISSN: 2582-6433

DIGITAL FACES, REAL HARMS: DEEPFAKES, PERSONALITY RIGHTS, AND THE EMERGING LAW OF AI-GENERATED IDENTITY HARM

AUTHORED BY - SHAURYA CHAUHAN & BHUPENDRA YADAV
3rd Year
National Law Institute University, Bhopal

Abstract

Generative artificial intelligence has made it possible to put anyone's face on anyone's body, clone any voice with a few seconds of audio, and fabricate a statement no one ever made. This is not science fiction. It is a daily reality for millions of people in India, and the law is still struggling to catch up. This paper looks closely at how Indian courts have responded to the deepfake problem in the absence of dedicated legislation, tracing the evolution of personality rights doctrine through three landmark Delhi High Court decisions: Anil Kapoor v Simply Life India (2023), Jackie Shroff v The Peppy Store (2024), and Sadhguru Jagadish Vasudev v Igor Isakov (2025). It then places those decisions in comparative context, examining how the US, EU, UK, China, and Denmark have approached the same problem, and critically evaluates India's IT (Intermediary Guidelines)

Amendment Rules, 2025, which represent the country's first statutory attempt to regulate synthetic media. The paper argues that while judicial improvisation has filled the immediate gap admirably, what India actually needs is a dedicated Personality Rights Act, a comprehensive AI harm chapter in the forthcoming Digital India Act, and institutional infrastructure in the form of a National Deepfake Detection Lab.

I. Introduction

In November 2023, a deepfake video of actress Rashmika Mandanna spread across Indian social media. The video showed her face superimposed onto another woman's body in sexually suggestive content. She had no knowledge of it, no involvement in it, and no immediate legal remedy available to her. By the time platforms acted, it had been watched millions of times. The incident prompted a government advisory and parliamentary debate, but produced no

ISSN: 2582-6433

prosecution and no compensation for the victim.

That episode captures the core problem this paper addresses. Deepfake technology has moved faster than the law. Tools that once required specialist expertise and serious computing resources are now available as free mobile applications. A convincing voice clone can be produced from thirty seconds of audio. A face swap can be generated in minutes. The harms this enables range from the devastatingly personal (non-consensual intimate imagery) to the commercially damaging (fake celebrity endorsements) to the politically destabilising (fabricated statements by public figures).

India's response has been characterised by creative judicial action in a legislative vacuum. In the absence of a personality rights statute, the Delhi High Court has improvised using constitutional law, tort doctrine, intellectual property principles, and the Information Technology Act, 2000. The result is an impressive body of judge-made law, but one that is fragile, inconsistent in its doctrinal foundations, and simply out of reach for the vast majority of deepfake victims who are not celebrities with the resources to litigate.

This paper examines that judicial response in detail, compares it with approaches taken in other jurisdictions, and asks what India would need to do to move from improvised protection to a coherent framework. Part II explains how deepfakes work and why they present difficulties that existing legal tools were not designed to handle. Part III analyses the three landmark cases. Part IV examines the doctrinal foundations those cases drew upon. Part V surveys the global landscape. Part VI evaluates India's 2025 regulatory rules and proposes three legislative reforms.

II. Understanding Deepfakes: Technology, Taxonomy, and Harm

A. How the Technology Works

Deepfakes are created using machine learning models, principally Generative Adversarial Networks (GANs) and, more recently, diffusion models. In a GAN, two neural networks compete with each other: one tries to generate synthetic content convincing enough to be mistaken for real, while the other tries to detect what is synthetic. Over time, the generator gets very good at its job. Diffusion models work differently, starting with noise and gradually shaping it toward a target output, but they achieve similarly realistic results and have become the dominant architecture in the most widely used consumer-facing tools.

ISSN: 2582-6433

Three features of this technology create particular difficulty for the law. First, accessibility: tools capable of producing convincing deepfakes are freely available as apps and open-source code, with no technical barrier to entry. Second, scalability: a single person can produce thousands of images or hours of video at near-zero marginal cost, overwhelming both platform moderation systems and the individual takedown process. Third, detection limits: the best available detection tools operate at about 65 to 70 per cent accuracy, in an adversarial dynamic where generation and detection capabilities improve together. A court that relies on forensic detection evidence in deepfake litigation needs to understand these limits.

B. The Range of Harms

The harms deepfakes cause vary considerably, and any legal framework needs to account for that variation. The largest category by volume is non-consensual intimate imagery: research consistently shows that over 90 per cent of deepfake videos circulating online are of this kind, and women make up the vast majority of victims. The harm is primarily dignitary and psychological, though professional and social consequences frequently follow.

The second category is false endorsement and commercial fraud. A deepfake video of a celebrity apparently recommending a cryptocurrency scheme or a fraudulent financial product exploits the victim's reputation to deceive consumers. This is both an economic harm (the celebrity's endorsement value is exploited without payment or consent) and a reputational one (the celebrity is associated with fraud). The third category is electoral manipulation. India's 2024 general elections saw multiple deepfake incidents, including a video falsely depicting a senior government minister making controversial statements about reservation policy.

III. The Landmark Indian Cases

A. Anil Kapoor v Simply Life India and Others (Delhi HC, 2023)

Background. Anil Kapoor filed a civil suit against sixteen defendants who had been exploiting his identity in a variety of ways: deepfake videos placing his face on Disney characters and other celebrities; AI-generated content falsely suggesting he endorsed various products and services; ringtones and GIF files replicating his voice and dialogue; websites charging fees for services falsely attributed to him; pornographic content using his likeness; and domain names incorporating his name without authorisation. He sought an ex parte injunction, and Justice Prathiba M. Singh heard the application in September 2023.

What the Court Decided. The court granted what is effectively an omnibus injunction, restraining not only the named defendants but the world at large from using Kapoor's name,

ISSN: 2582-6433

image, voice, likeness, or persona in any form, and from deploying AI tools, face-morphing technology, or any other digital mechanism to replicate those attributes for commercial purposes. It directed domain name registrars to suspend infringing domains, and asked the Department of Telecommunications and MeitY to cooperate in enforcement.

Why It Matters. This is the first Indian judgment to specifically identify AI-generated deepfakes as a violation of personality rights. The court held plainly that the use of AI, machine learning, deepfakes, and face-morphing technology to create unauthorised content for commercial gain constitutes a violation of personality rights. It also issued the first in rem John Doe order in India for personality rights: an injunction directed not at specific named parties but at anyone in the world who might engage in the prohibited conduct. The court drew on R Rajagopal v State of Tamil Nadu (1994) for the constitutional privacy foundation, and on American decisions including Vanna White v Samsung Electronics America (1992) for the right of publicity framework.

Points of Critique. Two aspects of the Anil Kapoor order deserve scrutiny. The first is the link the court drew between personality rights and the constitutional right to livelihood under Article

21. This is doctrinally ambitious: constitutional rights in India are generally understood to operate against the state, and reading a commercial celebrity's publicity right into Article 21 stretches the provision considerably. The second concern is the breadth of the in rem order: an injunction against

the world at large, without any judicial assessment of whether particular expressive uses of the Plaintiff's persona are legitimate, raises obvious free speech questions. The subsequent Jackie Shroff decision partially addressed this, but the broader tension remains.

B. Jackie Shroff v The Peppy Store and Others (Delhi HC, 2024)

Background. Jackie Shroff's suit covered a wider variety of defendants than the Kapoor case: e- commerce platforms selling merchandise with his image, a YouTube creator who had made a compilation video of his interviews under the title 'Jackie Shroff Is Savage, Thug Life!', other channels publishing distorted or derogatory compilations, a platform offering ringtones and wallpapers, and, most significantly for present purposes, an operator running a commercial AI chatbot built around attributes of his persona. The suit also sought protection for the word 'Bhidu', a colloquial term so closely associated with Shroff as to have become a registered trademark and, the Plaintiff argued, a personality attribute in itself.

The AI Chatbot Holding. Justice Sanjeev Narula granted an injunction against the AI chatbot

ISSN: 2582-6433

operator. This is the first time an Indian court has specifically restrained an AI chatbot on personality rights grounds. The logic of the holding is clear: if you commercially deploy a chatbot that is essentially designed to impersonate a real, identifiable celebrity, you are exploiting that person's personality attributes without consent, and that is an infringement regardless of whether the chatbot produces literal copies of any protected work.

The Free Speech Analysis. The court declined to restrain the 'Thug Life' compilation video, finding it to be a form of artistic commentary rather than commercial exploitation. This is the most important doctrinal contribution of the Jackie Shroff judgment. The court drew a clear line: using a celebrity's persona for commercial gain is prohibited, but using publicly available content about a celebrity to create commentary, parody, or meme-style expression is protected. This distinction is essential if personality rights law is not to become a tool for celebrities to suppress legitimate public discussion and creative expression about themselves.

Doctrinal Tension With Anil Kapoor. The Jackie Shroff court was noticeably more cautious than the Anil Kapoor bench about grounding personality rights in Article 21's livelihood guarantee. Justice Narula did not adopt the constitutional framing with the same enthusiasm, leaving open the question of whether the Indian right of publicity is a constitutional right, a property right, a common law tort, or some combination of the three. This divergence between two benches of the same court on an unsettled question illustrates exactly why legislative intervention is needed.

C. Sadhguru Jagadish Vasudev v Igor Isakov and Others (Delhi HC, 2025)

Background. This case presented a more technically sophisticated version of the problem. The defendants were largely anonymous operators of rogue overseas websites who had been using AI- generated deepfakes of Sadhguru's voice, face, and distinctive appearance to circulate fabricated content, including fake videos claiming he had been arrested and fake endorsements of commercial products. Standard takedown procedures had failed because the harm was disseminated too quickly and the operators too well-concealed to be reached through conventional means.

The Technological Remedy. Justice Saurabh Banerjee's response was to go beyond the conventional injunction. The court ordered platform operators, including YouTube, to deploy automated AI-based detection systems capable of identifying and removing identical infringing content, with a compliance deadline of 36 hours from detection. This is something no other court in the world had done. Rather than simply restraining specific conduct, the court required technology to respond to technology: a platform benefiting from AI tools that disseminate

ISSN: 2582-6433

deepfakes at scale must deploy AI tools to detect and remove them at scale.

Significance and Open Questions. Justice Banerjee's observation that 'the rights of a plaintiff cannot be rendered otiose in this world of rapidly developing technology' captures the spirit of this decision well. The court was unwilling to accept that deepfake harm was simply the price of living in the digital age. However, the order raises a real question about the intermediary liability framework under Section 79 of the IT Act: if a platform is ordered to proactively monitor for specific content, does it lose its passive-conduit status and face enhanced liability for other harmful content it fails to catch? The court did not address this tension, and it will need to be resolved before this kind of structural remedy becomes routine.

IV. Doctrinal Foundations

A. Article 21 and Constitutional Privacy

The constitutional anchor for personality rights in India is Article 21, read expansively by the Supreme Court in KS Puttaswamy v Union of India (2017). The nine-judge bench in Puttaswamy held that the right to privacy encompasses informational privacy, the right to control one's own narrative, and decisional autonomy over personal matters. A deepfake places someone's face on content they never made and attributes to them statements they never uttered. It would be strange if this did not engage a constitutional right to control one's own narrative. The Delhi High Court's personality rights decisions have exploited this opening, though the application of constitutional rights against private parties remains doctrinally complex.

B. The Common Law of Passing Off

Indian courts have most consistently grounded personality rights claims in the law of passing off. The classic formulation requires three elements: goodwill in a name or identity, a misrepresentation by the defendant that creates confusion about endorsement or association, and damage to that goodwill. The Delhi High Court's 2010 decision in DM Entertainment Pvt Ltd v Baby Gift House established that a celebrity's distinctive characteristics generate protectable goodwill in this sense. A deepfake endorsement video is a textbook misrepresentation of commercial association. The limitation of this approach is that passing off is ill-suited to non- commercial deepfake harm: a fabricated intimate image does not involve any misrepresentation of commercial association and causes primarily dignitary rather than economic damage.

ISSN: 2582-6433

C. Performers' Rights Under the Copyright Act

Sections 38, 38A, and 38B of the Copyright Act, 1957 protect performers in their live performances for fifty years from fixation. Moral rights under Section 38B include the right to object to modifications of a performance that are prejudicial to the performer's reputation. An AI system trained to clone a particular singer's voice, or to replicate an actor's distinctive delivery, directly engages these provisions. The Bombay High Court's 2024 interim order protecting Arijit Singh's voice against commercial AI replication rested partly on this ground. The limitation is that Section 38's performers' right is confined to the performance itself, not to the full range of personality attributes that a deepfake can replicate.

D. The Information Technology Act, 2000

Sections 66C (identity theft), 66D (cheating by personation using computer resources), 66E (privacy violation through publication of intimate images), and 67A (obscene electronic content) are the primary IT Act provisions invoked in deepfake cases. The Bharatiya Nyaya Sanhita, 2023 adds further criminal provisions. The difficulty with all of these is that they were drafted for a world without generative AI and their application requires significant interpretive effort. Section 66E, for instance, refers to images of a 'private area': it does not obviously cover a deepfake in which the victim's face is placed on someone else's body in a non-private context. Courts have been willing to stretch these provisions, but the stretching creates uncertainty and limits the availability of remedies.

V. The Global Picture

A. United States: The Property Model

The US has the most developed right of publicity law in the world, though it exists at state level rather than federally. California and New York both protect individuals from commercial exploitation of their name, likeness, voice, and signature. The right is understood as a property right: alienable, descendible, and commercially licensable. This gives it considerable strength in false endorsement cases, but less traction in non-commercial deepfake harm. Tennessee's ELVIS Act, enacted in 2024, is the first US statute specifically addressing AI voice cloning: it requires consent before creating a digital replica of a performer's voice for commercial purposes and extends the right to performers' estates. At the federal level, the TAKE IT DOWN Act, signed in April 2025, criminalises non-consensual intimate deepfake imagery and requires platforms to remove such content within 48 hours of notification. The proposed No Fakes Act would create a federal right of publicity covering digital replicas, but it remains pending in the

ISSN: 2582-6433

Senate as of early 2026.

B. European Union: The Dignity Model

The EU's approach reflects its characteristic emphasis on dignity and privacy rather than property. The GDPR classifies biometric data as special category data requiring explicit consent for processing. Creating a deepfake necessarily involves processing the biometric data of the person whose face or voice is replicated, giving data protection authorities a powerful tool that applies to everyone, not just celebrities. The EU AI Act, in force since August 2024, adds a transparency layer: AI-generated synthetic content must be labelled as such, and providers of general-purpose AI models must maintain technical documentation enabling attribution. The Act also prohibits certain applications outright, including real-time remote biometric identification in public spaces. The EU withdrew its proposed AI Liability Directive from its legislative programme in 2025, leaving civil liability to national law and the Product Liability Directive.

C. United Kingdom: A Work in Progress

The UK has a collection of relevant laws rather than a coherent framework. The Online Safety Act, 2023 makes it a criminal offence to share non-consensual intimate deepfake images. The Data Protection Act, 2018 carries GDPR standards into domestic law. But there is no statutory right of publicity analogous to the US model, and the common law tools available to victims are imperfectly suited to deepfake harm. The Law Commission is reviewing synthetic media law, with a report expected in 2026.

D. China: The Prescriptive Model

China has the most prescriptive global framework. Its Deep Synthesis Provisions, effective from 2023 and updated in September 2025, require providers of deep synthesis technology to implement real-name verification, obtain consent before processing any individual's biometric data, label all synthetic content with visible and invisible watermarks, maintain generation logs for fifteen years, and refuse service for content that violates the rights of others. The model is notable for its mandatory watermarking requirements and pre-market compliance obligations, aspects of which are reflected in India's 2025 Rules.

E. Denmark: Treating the Body as Property

Denmark has proposed what may be the most radical approach: amendments to copyright law

ISSN: 2582-6433

that would treat each person's body, facial features, and voice as their intellectual property, giving them the right to demand the takedown of any deepfake of their likeness without needing to prove harm. This reframes the entire question: instead of asking whether a deepfake violates privacy or misrepresents commercial association, it simply asks whether someone else's likeness was used without consent. It is a clean and powerful rule, and one that countries like India, which need to protect both celebrities and ordinary people, might consider seriously.

VI. India's IT Amendment Rules, 2025: What They Do and What They Miss

A. The Rules

MeitY notified the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025 on 15 November 2025. They provide India's first statutory definition of synthetic media: information that is artificially or algorithmically created, generated, modified, or altered using a computer resource in a manner that appears reasonably authentic or true. The main obligations are that platforms enabling creation of synthetic content must embed permanent unique identifiers or metadata in all such content; labels must cover at least 10 per cent of the visual area or the first 10 per cent of audio duration; significant social media intermediaries (over five million registered users) must adopt tools to verify whether content uploaded by users is synthetic; and users are required to declare whether content they upload is AI-generated.

B. What the Rules Get Right

It is worth being fair about what the 2025 Rules actually achieve. They provide the first legislative definition of synthetic media, which matters enormously: courts no longer have to improvise a definition when they encounter a deepfake case, and the definition itself is broadly and sensibly drafted. The mandatory labelling regime creates a forensic trail that did not exist before. The proportionate obligations model, imposing heavier duties on large platforms than on small ones, follows sound regulatory practice. And the clarification that proactive content removal does not risk a platform's Section 79 safe harbour removes a significant disincentive for platforms to act.

C. The Gaps

That said, the Rules have real limitations. The most significant is that they address labelling without addressing liability. They tell platforms what to do but say nothing about the civil or criminal responsibility of the person who creates a harmful deepfake. A victim who suffers

ISSN: 2582-6433

reputational or economic harm from a deepfake still has no direct statutory cause of action against its creator: they must fall back on the IT Act's pre-AI provisions, the general law of tort, or the criminal law, none of which was designed for this situation.

There is also a constitutional question. The Rules are subordinate legislation made under the parent IT Act, 2000. The obligations they impose, particularly mandatory metadata embedding and user verification, go significantly beyond the safe harbour framework in Section 79, and it is not obvious that the delegated legislative power in the parent Act extends to these requirements. This creates a vulnerability that platforms seeking to resist compliance might exploit.

Finally, the enforcement mechanism does not match the speed of the harm. Deepfake damage is concentrated in the first 24 to 72 hours: a fabricated video that goes viral over a weekend causes most of its harm before any officer of Joint Secretary rank has seen a complaint. Building a regulatory framework around officers of that seniority approving takedowns is not a design calibrated to the speed of digital harm.

D. What India Actually Needs

Three legislative steps would substantially close the gap. First, a Personality Rights and Digital Identity Act that codifies the right of publicity as a statutory right available to all natural persons, not just celebrities. The Act should define protectable attributes to include name, image, voice, biometric features, and distinctive mannerisms, and specify clear defences for satire, parody, research, journalism, and education. It should create a direct civil cause of action against anyone who creates or distributes a deepfake of another person without consent, with graduated remedies including injunctions, damages, and account of profits.

Second, the forthcoming Digital India Act, which is expected to replace the IT Act, 2000, should contain a dedicated chapter on AI-generated harm. This chapter should codify the deployer-as- principal rule that is emerging from Indian and international case law (see Moffatt v Air Canada [2024] BCCRT 149 for the clearest articulation): the commercial deployer of an AI system whose outputs violate personality rights bears primary liability, subject to a defence of user misuse. It should also require consent for AI voice cloning and likeness replication, and create a rapid-relief tribunal that can grant emergency injunctions within hours rather than weeks.

Third, India should establish a National Deepfake Detection Lab under MeitY and CERT-In, with a mandate to develop and make publicly available detection tools, maintain a national deepfake incident registry, and provide forensic support to courts and law enforcement. The

ISSN: 2582-6433

scale of the problem, documented by NASSCOM as over 120,000 AI-generated deepfakes per month in India alone, requires institutional infrastructure, not just individual judicial remedies.

VII. Conclusion

Reading through these three judgments, one is struck by how much the Delhi High Court has managed to construct from very little. In the absence of a personality rights statute, in the absence of dedicated deepfake legislation, working only with constitutional doctrine, common law, IP provisions designed for a different era, and a broad equitable jurisdiction, Indian courts have arrived at rules that are broadly sensible: commercial exploitation of someone's AI-replicated identity requires consent; AI chatbots built around a celebrity's persona are not exempt; platforms may be required to use technology to combat the technological harms they enable; but memes and parody and artistic commentary on public figures remain protected. These are good rules. The problem is that they are good rules produced by improvisation, and improvisation is not the same as a framework.

The IT Amendment Rules, 2025 are a real step forward, but they are a step toward a framework, not the framework itself. They address the labelling problem without addressing the liability problem. They tell platforms to label synthetic content without telling anyone what happens when a deepfake destroys someone's life. That is a gap Parliament needs to fill.

India has the judicial infrastructure, the policy intent, and the legislative vehicle in the forthcoming Digital India Act. It has a judiciary that has shown it will not wait indefinitely for Parliament to act. What is needed now is for Parliament to act, and to act with sufficient precision that the protection reaches not only the celebrities who can afford to litigate but the millions of ordinary people who cannot.

Footnotes

1. Anil Kapoor v Simply Life India and Ors CS(COMM) 652/2023 and IA 18237/2023 to 18243/2023 (Delhi High Court, 20 September 2023).
2. Jaikishan Kakubhai Saraf alias Jackie Shroff v The Peppy Store and Ors CS(COMM) 389/2024, 2024 SCC OnLine Del 3664 (Delhi High Court, 15 May 2024).
3. Sadhguru Jagadish Vasudev and Anr v Igor Isakov and Ors CS(COMM) 578/2025, 2025 SCC OnLine Del 3804 (Delhi High Court, 30 May 2025).
4. R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632.
5. KS Puttaswamy v Union of India (2017) 10 SCC 1.
6. DM Entertainment Pvt Ltd v Baby Gift House 2010 SCC OnLine Del 4790.
7. Arijit Singh v Codible Ventures LLP 2024 SCC OnLine Bom 2445 (Bombay High Court, July 2024).
8. IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025, notified 15 November 2025.

ISSN: 2582-6433

9. TAKE IT DOWN Act Pub L No 119 (signed April 2025).
10. Tennessee ELVIS Act Tenn Code Ann ss 47-25-1101 et seq (2024).
11. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence [2024] OJ L 1689 (EU AI Act), in force 1 August 2024.
12. Provisions on the Administration of Deep Synthesis Internet Information Services (China), updated September 2025.
13. Online Safety Act 2023 (UK).
14. Moffatt v Air Canada [2024] BCCRT 149.
15. NASSCOM, Deepfake Threat Report (2024).
16. World Economic Forum, Global Risks Report 2024.
17. Vanna White v Samsung Electronics America Inc 971 F 2d 1395 (9th Cir 1992).
18. Rajat Sharma v Union of India WP(C) No 6560 of 2024 (Delhi High Court, 2024).
19. Record of Law, 'Regulating AI and the Internet in India: Challenges of Deepfakes and Personality Rights' (Record of Law, 26 August 2025) <recordoflaw.in> accessed 15 March 2026.
20. Khurana and Khurana, 'Deepfake Regulation India 2025: MeitY's Comprehensive IT Rules Amendment' (Mondaq, December 2025) <mondaq.com> accessed 15 March 2026.

Select Bibliography

Cases

Anil Kapoor v Simply Life India and Ors CS(COMM) 652/2023 (Delhi HC 2023). Arijit Singh v Codible Ventures LLP 2024 SCC OnLine Bom 2445 (Bombay HC 2024). DM Entertainment Pvt Ltd v Baby Gift House 2010 SCC OnLine Del 4790.

Jackie Shroff v The Peppy Store and Ors CS(COMM) 389/2024 (Delhi HC 2024). KS Puttaswamy v Union of India (2017) 10 SCC 1.

Moffatt v Air Canada [2024] BCCRT 149.

R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632.

Sadhguru Jagadish Vasudev v Igor Isakov and Ors CS(COMM) 578/2025 (Delhi HC 2025).

Vanna White v Samsung Electronics America Inc 971 F 2d 1395 (9th Cir 1992).

Legislation and Regulation

Bharatiya Nyaya Sanhita 2023 (India). Copyright Act 1957 (India).

Digital Personal Data Protection Act 2023 (India). Information Technology Act 2000 (India).

IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2025 (India).

Online Safety Act 2023 (UK).

Provisions on the Administration of Deep Synthesis Internet Information Services (China 2023, updated 2025).

Regulation (EU) 2024/1689 (Artificial Intelligence Act). TAKE IT DOWN Act 2025 (US).

Tennessee ELVIS Act Tenn Code Ann ss 47-25-1101 et seq (2024).

Secondary Sources

BananaIP Intellepedia, 'Safeguarding Digital Identity in the Age of Deepfakes' (January 2026).

ISSN: 2582-6433

Khurana and Khurana, 'Understanding the Relevance of the Anil Kapoor vs Simply Life India Case' (February 2025).

Law.asia, 'India Tightens Rules on Deepfakes and AI-Generated Content' (November 2025).

NASSCOM, Deepfake Threat Report (2024).

Record of Law, 'Regulating AI and the Internet in India: Challenges of Deepfakes and Personality Rights' (August 2025).

SpicyIP, 'After Anil Kapoor, Jackie Shroff Follows Suit' (May 2024). World Economic Forum, Global Risks Report 2024.