

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

DEEPAKES AND CRIMINAL LIABILITY IN INDIA: EXAMINING THE NEED FOR A COMPREHENSIVE LEGAL FRAMEWORK

AUTHORED BY - ATUL VERMA

ABSTRACT

The proliferation of generative adversarial networks and diffusion-based synthesis tools has made the fabrication of hyper-realistic audio, image, and video content — popularly termed “deepfakes” — cheap, fast, and accessible to lay users. India, home to the world’s largest base of internet and social-media users, has witnessed a sharp rise in deepfake-enabled harms: non-consensual sexual imagery, celebrity impersonation for commercial fraud, voice-cloned financial scams, and synthetic political content circulated during electorally sensitive periods. This paper undertakes a doctrinal and analytical examination of the adequacy of India’s existing criminal law architecture — principally the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 as amended in 2026 — to address deepfake-enabled criminality. It traces the judicial response of Indian High Courts, particularly the Delhi and Bombay High Courts, which have fashioned an ad hoc jurisprudence of “personality rights” and John Doe (Ashok Kumar) injunctions in the absence of a dedicated statute. The paper argues that the prevailing legal response is reactive, fragmented, and predominantly civil/regulatory in character, leaving significant gaps in mens rea attribution, evidentiary authentication, cross-border enforcement, and platform accountability for criminal (as opposed to merely unlawful) content. Employing a doctrinal methodology supported by case analysis and comparative reference to the European Union’s AI Act and the United States’ state-level deepfake statutes, the paper identifies four structural deficits in Indian law: (i) absence of a deepfake-specific offence with calibrated mens rea thresholds; (ii) inadequate authentication and chain-of-custody standards for synthetic media evidence; (iii) an intermediary liability regime skewed toward takedown speed rather than investigative cooperation; and (iv) the absence of a victim-centric compensatory mechanism independent of civil suit. The paper concludes with a set of drafting recommendations for a standalone “Digital Impersonation and Synthetic Media (Prevention) Act” that would consolidate existing provisions, introduce graded offences, and harmonise the 2026 IT Rules

with the criminal justice trilogy (BNS, BNSS, BSA).

Keywords: *Deepfakes; Synthetically Generated Information; Criminal Liability; Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Personality Rights; Intermediary Liability; Digital Evidence; Artificial Intelligence Regulation; Privacy Law*

1. INTRODUCTION

The term “deepfake”, a portmanteau of “deep learning” and “fake”, refers to synthetic media in which a person’s likeness, voice, or actions are digitally fabricated or altered using machine-learning techniques — principally generative adversarial networks (GANs), autoencoders, and, more recently, diffusion models — to produce content that a reasonable viewer would perceive as authentic.¹

India’s exposure to this technology is disproportionately high. With over 850 million internet users and the world’s largest consumer base for short-form video and messaging applications, the marginal cost of producing and disseminating a convincing deepfake in India has fallen dramatically. The Ministry of Electronics and Information Technology (“MeitY”) itself has acknowledged that deepfakes pose a “direct threat to the trust deficit created by misinformation and disinformation powered by deepfakes.”²

The harms are neither speculative nor confined to celebrity culture. India has recorded a rapidly diversifying set of deepfake-enabled criminal patterns: (a) non-consensual sexually explicit imagery of private individuals, overwhelmingly targeting women; (b) voice-cloned “digital arrest” and family-emergency frauds in which synthetic audio of a relative or a senior police/judicial officer is used to extort money; (c) synthetic endorsements attributing statements or product recommendations to film and public personalities without consent; and (d) synthetic political content — fabricated speeches, manipulated rally footage — timed to elections and communal flashpoints.

Two doctrinal features distinguish deepfakes from earlier forms of digital forgery or morphing.

¹Robert Chesney & Danielle Citron, ‘Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security’ (2019) 107 California Law Review 1753, 1758–60.

²Ministry of Electronics and Information Technology, Government of India, Advisory on Due Diligence to be Observed by Intermediaries under the Information Technology Act, 2000 and Rules thereunder (26 December 2023).

First, the underlying technology is generative rather than merely manipulative: it does not alter an existing photograph but synthesises new, non-existent visual or auditory data conditioned on a dataset of the victim's real appearance or voice. Second, the marginal cost of production has collapsed to near zero, converting what was once a specialised forensic-grade skill into a consumer-app function.³

India has, until very recently, possessed no statute that defines “deepfake” as a legal term of art. Prosecutions and civil suits have instead proceeded through a patchwork of provisions originally drafted for unrelated mischief: identity theft and cyber-impersonation offences under the Information Technology Act, 2000 (“IT Act”); forgery, cheating, and defamation offences inherited (with modification) from the Indian Penal Code, 1860 into the Bharatiya Nyaya Sanhita, 2023 (“BNS”); and evidentiary provisions under the Indian Evidence Act, 1872, now replaced by the Bharatiya Sakshya Adhiniyam, 2023 (“BSA”). It was only with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (“IT Amendment Rules, 2026”), notified on 10 February 2026 and effective from 20 February 2026, that Indian law for the first time defined “synthetically generated information” (“SGI”) as a distinct regulatory category.

1.1 Statement of the Problem

The absence, until 2026, of a definitional anchor for synthetic media in Indian criminal law produced two connected difficulties. First, prosecutors were compelled to force deepfake conduct into offence definitions built around physical or documentary forgery, non-consensual capture of images, or personation using stolen credentials — categories that do not neatly capture the wholly generative character of AI-synthesised content. Second, courts confronting urgent, high-profile harms (particularly against film and public personalities) responded through civil injunctive relief — in personam and in rem “John Doe” orders grounded in an evolving common-law right of personality — rather than through the criminal process, leaving the deterrent and punitive dimension of the law comparatively underdeveloped.

1.2 Objectives of the Study

- To map the existing statutory and regulatory provisions in India that bear, directly or indirectly, on deepfake-enabled criminal conduct.

³Danielle Citron, ‘How Deepfakes Undermine Truth and Threaten Democracy’ TED (2019); see also Bobby Chesney and Danielle Citron (n 1) 1772.

- To critically analyse the judicial response of Indian High Courts to deepfake and personality-rights litigation between 2022 and 2026.
- To evaluate the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 as a regulatory (as opposed to criminal) response to synthetic media harms.
- To identify structural and doctrinal gaps in the attribution of criminal liability for AI-generated harms, including questions of mens rea, intermediary complicity, and cross-border enforcement.
- To recommend the contours of a comprehensive, rights-respecting legislative framework specific to deepfakes and synthetic media.

1.3 Research Questions

- Does the existing criminal law of India — the IT Act, 2000 and the BNS, 2023 — adequately capture the distinctive harms caused by AI-generated synthetic media?
- Has judicial innovation through personality-rights jurisprudence substituted for, or merely supplemented, the need for criminal legislative reform?
- Does the IT Amendment Rules, 2026 regime adequately bridge the gap between platform-level regulation and individual criminal liability?
- What legislative model would best balance deterrence of deepfake-enabled crime against the constitutional guarantees of free speech and innovation under Articles 19(1)(a) and 19(1)(g)?

1.4 Research Methodology

This paper adopts a doctrinal legal research methodology, involving the analysis of primary legal sources (statutes, delegated legislation, and case law) and secondary sources (peer-reviewed journal articles, law-firm commentary, and government advisories). Case law is analysed using the traditional common-law method of ratio extraction, supplemented by a comparative lens drawing on the European Union's Artificial Intelligence Act, 2024 and selected United States state-level deepfake statutes (California, Texas, and Virginia) to test the adequacy of the Indian framework against international regulatory benchmarks. Given the doctrinal nature of the inquiry, the paper relies on reported judicial orders and secondary legal literature rather than primary empirical fieldwork; quantitative figures on litigation trends presented in this paper (see Figure 3) are therefore illustrative approximations compiled from reported High Court orders discussed herein, not official judicial statistics.

1.5 Scope and Limitations

The paper confines itself to criminal and quasi-criminal liability under Indian law; it engages with civil personality-rights litigation only to the extent that such litigation illuminates the adequacy (or otherwise) of the criminal framework. Intellectual property questions concerning the copyrightability of AI-generated content, and data-protection questions under the Digital Personal Data Protection Act, 2023 that are not directly tied to criminal liability, are addressed only briefly. The analysis is current to August 2026 and reflects the IT Amendment Rules, 2026 as the most recent regulatory intervention.

2. LITERATURE REVIEW

Scholarship on deepfakes has evolved through three broadly identifiable phases, mirrored in both international and Indian legal writing.

2.1 First Phase: Technological Description and Democratic Harms (2018–2020)

Early foundational scholarship, most notably Chesney and Citron's widely cited article, framed deepfakes primarily as a threat to democratic discourse, national security, and individual privacy, cataloguing potential harms without yet confronting the doctrinal question of criminal attribution in any particular jurisdiction.⁴

Citron's subsequent work extended this analysis to the specific harm of non-consensual synthetic pornography, arguing that existing revenge-pornography statutes in most jurisdictions were drafted around the unauthorised distribution of genuine images and therefore failed to capture wholly fabricated content.⁵

2.2 Second Phase: Comparative Regulatory Responses (2020–2023)

A second wave of scholarship undertook comparative analysis of early legislative responses, principally in the United States, where several states (California, Texas, Virginia) enacted narrow deepfake statutes targeting election-related and sexual synthetic content, and in the European Union, where the draft Artificial Intelligence Act proposed transparency obligations (labelling) for AI-generated content rather than criminalisation per se.⁶

Indian scholarship during this period was comparatively sparse and largely descriptive,

⁴Chesney and Citron (n 1) 1760–75.

⁵Danielle Keats Citron, 'Sexual Privacy' (2019) 128 Yale Law Journal 1870, 1917–22.

⁶Rebecca Delfino, 'Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act' (2019) 88 Fordham Law Review 887; European Commission, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act) COM(2021) 206 final, art 52.

cataloguing the applicability of Sections 66C, 66D, 66E, 67, and 67A of the IT Act, 2000 to deepfake conduct without empirical or doctrinal depth, and frequently concluding — correctly, in the present author’s assessment — that these provisions were “not crafted for the nuances of synthetic media.”

2.3 Third Phase: Post-BNS and Post-2026 Rules Scholarship

The coming into force of the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023 on 1 July 2024, followed by the IT Amendment Rules, 2026, has generated a third and still-emerging wave of Indian scholarship. This literature is divided between (a) commentary welcoming the SGI regime as a decisive regulatory intervention, and (b) more critical doctrinal work arguing that the 2026 Rules — being delegated legislation confined to intermediary due diligence under Section 79 of the IT Act — cannot, by themselves, create new criminal offences or cure the mens rea and attribution deficits in the BNS and IT Act.⁷

On the judicial side, case-comment literature has closely tracked the Delhi High Court’s personality-rights jurisprudence beginning with *Amitabh Bachchan v Rajat Nagi* and extending through *Anil Kapoor v Simply Life India*, *Jackie Shroff v The Peppy Store*, and the 2025–2026 line of orders protecting Aishwarya Rai Bachchan, Abhishek Bachchan, Karan Johar, and Sri Sri Ravi Shankar. Commentators are broadly united in treating this line of cases as judicial gap-filling — a common-law personality right assembled from Article 21 privacy jurisprudence (*Justice K.S. Puttaswamy v Union of India*), Sections 38 and 38A of the Copyright Act, 1957 (performers’ rights), and the tort of passing off — rather than as a substitute for criminal legislative reform.⁸

Most recently, commentary on the Supreme Court’s July 2026 remarks on ‘digital arrest’ and deepfake-enabled fraud has renewed calls for a standalone criminal statute, on the ground that voice-cloning and synthetic-video fraud continue to be prosecuted only through general extortion and cheating provisions of the BNS combined with Sections 66C and 66D of the IT Act — provisions the Court itself observed were ‘designed for an era before AI-generated synthetic video existed.’⁹

⁷See e.g. Vaish Associates Advocates, ‘Regulation of AI-Generated/Deepfake Content and Synthetically Generated Information (SGI) in India – New Rules’ (13 February 2026); cf. Legal Blur, ‘Deepfakes and Indian Law: Copyright & Liability’ (2026), arguing for a dedicated ‘Digital Identity and Personality Rights Act’.

⁸Candour Legal, ‘AI, Deepfakes, and Personality Rights in India: What Courts Are Doing Without a Statute’ (2026); Naik Naik & Co, ‘Delhi HC’s Protection to Anil Kapoor: A Landmark Order on Personality Rights’ (17 October 2023).

⁹See reporting on the Supreme Court of India’s observations on deepfake-enabled digital-arrest fraud (July 2026),

2.4 Research Gap

Existing Indian literature tends to treat the civil personality-rights track and the criminal/regulatory track as separate silos, and pre-2026 scholarship necessarily could not account for the IT Amendment Rules, 2026. This paper contributes an integrated analysis that (a) reads the 2026 SGI regime alongside the BNS/BSA criminal trilogy rather than in isolation; (b) evaluates whether civil John Doe injunctions have inadvertently reduced legislative pressure for criminal reform; and (c) proposes a specific legislative architecture rather than a general call for “comprehensive law.”

3. ANALYSIS AND DISCUSSION

3.1 The Pre-Existing Criminal Law Architecture

Prior to February 2026, India possessed no statute referencing “deepfake” or “synthetic media” by name. Prosecutions proceeded through a combination of provisions from the IT Act, 2000, and the BNS, 2023 (previously the Indian Penal Code, 1860), summarised in Table 1 below.

Table 1: Mapping of Deepfake-Enabled Conduct onto Pre-2026 Indian Criminal Provisions

Provision	Nature of Offence	Punishment	Fit for Deepfake Conduct
S.66C, IT Act, 2000	Identity theft — fraudulent or dishonest use of another’s electronic signature, password, or unique identification feature.	Up to 3 years + fine up to ₹1,00,000	Poor fit: presumes theft of an existing credential; a deepfake synthesises a new artefact rather than ‘using’ a stolen identifier.
S.66D, IT Act, 2000	Cheating by personation using a computer resource.	Up to 3 years + fine up to ₹1,00,000	Reasonably well-suited to fraud-oriented deepfakes (voice-cloned scams, fake executive video calls) but silent on non-fraudulent harms (defamation, non-consensual imagery).
S.66E, IT Act, 2000	Violation of privacy — capturing, publishing, or transmitting images of a	Up to 3 years + fine up to ₹2,00,000	Drafted around unauthorised capture of a real image; extension to wholly synthetic intimate imagery is an

discussed in Part 3.5 below.

	person's private area without consent.		interpretive stretch, not a natural fit.
Ss.67, 67A, IT Act, 2000	Publishing/transmitting obscene material (s.67) and sexually explicit material (s.67A) in electronic form.	Up to 3/5 years (first conviction) + fine	Applies well where deepfake content is sexual, but does not address non-sexual reputational, financial, or political deepfakes.
S.336, BNS, 2023	Forgery, including forgery of an electronic record.	Up to 7 years (aggravated forms)	Requires the making of a 'false document or electronic record' — courts must stretch the concept of a synthetically generated video to a 'false electronic record'.
Ss.316–318, BNS, 2023	Criminal breach of trust / cheating / cheating by personation.	Up to 7 years	Applicable to deepfake-enabled financial fraud; does not address non-financial harms.
S.356, BNS, 2023	Defamation.	Up to 2 years (simple imprisonment) / fine / both	Available where a deepfake damages reputation, but defamation is a relatively low-deterrence, often compoundable offence, and truth/good-faith defences complicate application to satire or parody deepfakes.
S.353, BNS, 2023	Statements conducing to public mischief (false/misleading information).	Up to 3 years	Potentially applicable to synthetic misinformation but requires proof of intent to cause specified public-order harms.
S.111, BNS, 2023	Organised crime (extended to cyber-organised crime).	5 years to life; death in terrorism-linked cases	Applicable only where deepfake production is linked to an organised syndicate — inapplicable to lone-actor harms, which are the majority of reported cases.

Source: Compiled by author from the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023.

The composite picture from Table 1 is one of doctrinal improvisation. No single provision was drafted with the generative, non-capture-based character of AI-synthesised media in view; each requires an interpretive analogy — treating a synthetic video as a ‘false electronic record’, or treating AI-based voice cloning as ‘personation’ — that Indian courts have, to their credit, generally been willing to draw, but that leaves considerable uncertainty regarding intent thresholds, especially for deepfakes created for satire, parody, or artistic expression that later cause unintended harm.

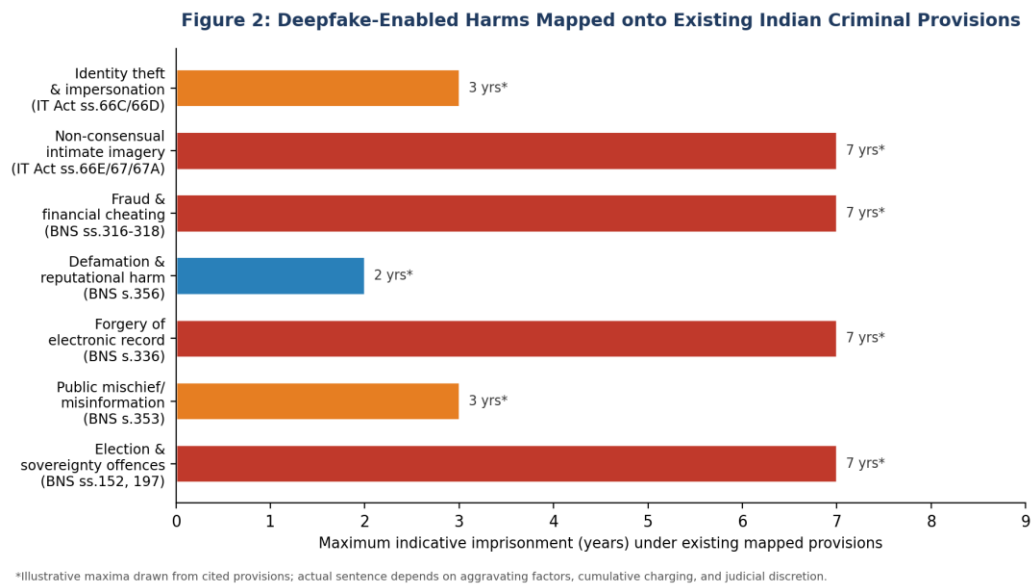


Figure 2: Deepfake-enabled harms mapped onto existing Indian criminal provisions, by illustrative maximum imprisonment.

3.2 The Constitutional Backdrop: Privacy and Personality

The doctrinal foundation for both the civil personality-rights jurisprudence and, indirectly, for arguments favouring criminalisation of non-consensual synthetic imagery, is the Supreme Court’s recognition of privacy as an intrinsic facet of the right to life and personal liberty under Article 21 of the Constitution in Justice K.S. Puttaswamy (Retd.) v Union of India.¹⁰

The Puttaswamy court held that any restriction on privacy must satisfy a three-fold test of legality, necessity, and proportionality — a standard that now frames the constitutional permissibility of both the IT Amendment Rules, 2026 takedown regime and any future criminal statute targeting deepfakes, insofar as such measures restrict speech under Article 19(1)(a) or trade/business under Article 19(1)(g). Any deepfake-specific offence must therefore be drafted with precision sufficient to survive an overbreadth or vagueness challenge, particularly given

¹⁰Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (nine-judge bench).

the risk that a poorly drafted ‘synthetic media’ offence could sweep in legitimate satire, parody, VFX, and AI-assisted creative work.

3.3 Judicial Gap-Filling: The Personality Rights Line of Cases

In the absence of criminal legislative specificity, the most consequential Indian judicial development between 2022 and 2026 has occurred on the civil side, through a rapidly expanding line of Delhi and Bombay High Court orders recognising a common-law ‘personality right’ and granting sweeping injunctive relief against deepfake misuse.

3.3.1 *Amitabh Bachchan v Rajat Nagi (Delhi HC, 2022)*

In this founding decision, the Delhi High Court granted an ad interim injunction operating in rem — binding not merely the named defendants but the world at large — restraining unauthorised commercial use of the actor’s name, voice, image, and likeness, including through AI-generated and morphed content. The Court reasoned that a celebrity’s persona carries independent commercial and dignitary value, the misappropriation of which constitutes an actionable wrong distinct from ordinary trademark or copyright infringement.¹¹

3.3.2 *Anil Kapoor v Simply Life India & Ors (Delhi HC, 2023)*

The Court went further in *Anil Kapoor*, granting an ex parte, omnibus injunction restraining sixteen named entities — and unknown persons at large — from using the actor’s name, image, voice, signature catchphrase (‘Jhakaas’), mannerisms, and dialogue delivery, expressly extending protection to AI-generated deepfakes, face-morphed GIFs, and NFT exploitation. This is frequently cited as the first Indian order to name AI/deepfake tools explicitly within the scope of an injunction.¹²

3.3.3 *The 2024–2026 Expansion*

Similar in rem orders have since issued in favour of Jackie Shroff (against unauthorised persona use, including a distinctive nickname), Sri Sri Ravi Shankar (against deepfake and morphed spiritual content), Karan Johar (against identity misuse in fraudulent online fundraising), Abhishek Bachchan, and Aishwarya Rai Bachchan, while the Bombay High Court has extended parallel protection to Akshay Kumar, Arijit Singh, Shilpa Shetty, Asha Bhosle, and Preity Zinta.¹³

¹¹*Amitabh Bachchan v Rajat Nagi & Ors*, CS(COMM) 819/2022 (Delhi High Court, 25 November 2022).

¹²*Anil Kapoor v Simply Life India & Ors*, CS(COMM) 652/2023 (Delhi High Court, 20 September 2023).

¹³See Candour Legal (n 12); Anantam IAS, ‘Delhi High Court Protects Personality Rights, Orders Removal of AI-Generated Fake Content’ (2026).

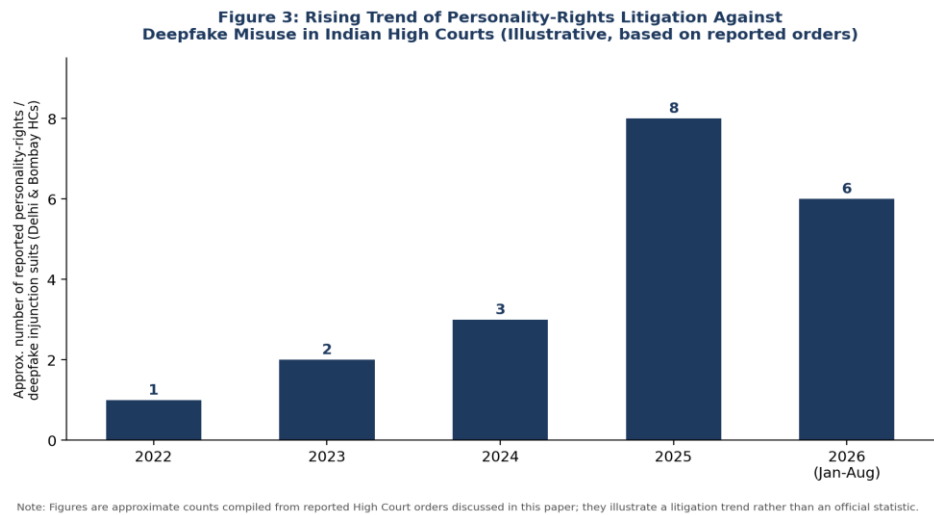


Figure 3: Illustrative growth in reported personality-rights/deepfake injunction suits before Indian High Courts, 2022–2026.

These orders share a common structural logic: reliance on the John Doe (or, in Indian practice, ‘Ashok Kumar’) device to bind unknown and future infringers; direction to the Department of Telecommunications and MeitY to issue blocking orders under Section 69A of the IT Act; and reliance on Section 79 safe-harbour principles to compel intermediary compliance rather than to impose direct criminal sanction on platforms.¹⁴

3.3.4 Critical Assessment

This civil jurisprudence deserves recognition as an important, judicially improvised stop-gap. It has three limitations, however, that this paper regards as central to the case for legislative reform. First, it is available in practice only to persons with the resources and public profile to litigate quickly in a constitutional court — predominantly film, sporting, and religious celebrities — and offers little accessible recourse to the private individual who is the more frequent victim of non-consensual intimate deepfakes or voice-cloned financial fraud. Second, an injunction, however broadly worded, is a civil remedy: it restrains future use and may ground a subsequent contempt action, but it does not itself impose criminal punishment proportionate to the culpability of the deepfake’s creator. Third, the personality-rights doctrine is itself judge-made and therefore lacks the definitional precision — particularly regarding mens rea, defences for satire/parody, and remedies for non-celebrities — that only primary legislation can supply.

¹⁴See Gulf News, ‘Delhi High Court Blocks AI Commercial Use of Bollywood Actor Anil Kapoor’s Image, Voice’ (22 September 2023); Anantam IAS (n 16).

3.4 Criminal Prosecutions: The Rashmika Mandanna Precedent

Criminal prosecution, as opposed to civil injunction, remains comparatively rare. The best-documented instance is the 2023 case involving a deepfake video morphing actress Rashmika Mandanna's face onto another woman's body, which went viral on social media. Delhi Police registered a case and arrested individuals involved in creating and disseminating the video under Sections 66D and 66E of the IT Act, 2000 — provisions targeting, respectively, cheating by personation and violation of privacy through capturing/publishing images without consent.¹⁵ The case is instructive precisely because of its provisional and improvised charge-sheet: Section 66E, which criminalises the capture or publication of a private image without consent, sits uneasily with a wholly AI-synthesised video in which no photograph of the victim's body was ever 'captured' in the statutory sense. The prosecution succeeded in securing arrests, but commentators have noted the doctrinal strain involved in applying a capture-based privacy offence to generative synthesis — precisely the gap this paper identifies as requiring legislative correction.

3.5 The Regulatory Response: IT Amendment Rules, 2026

The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (G.S.R. 120(E)), notified by MeitY on 10 February 2026 and effective from 20 February 2026, represent India's first legally operative definition of synthetic media. The Rules define 'synthetically generated information' (SGI) as information — audio, visual, or audio-visual — that is artificially or algorithmically created, generated, or modified using a computer resource in a manner that appears reasonably authentic or true, such that a reasonable person would be misled into believing it to be genuine.¹⁶

Substantively, the 2026 Rules impose four principal obligations on intermediaries: (a) mandatory, prominent labelling and permanent embedding of provenance metadata for SGI; (b) a tiered takedown regime — as short as two hours for the most invasive categories (non-consensual sexual SGI, SGI impersonating public officials for fraud) and up to seven days for other flagged SGI; (c) deployment of reasonable technical safeguards (automated classifiers) under new Rule 3(3) to detect and block specified categories of unlawful SGI before publication; and (d) a new Rule 2(1B) 'good samaritan' clause clarifying that good-faith

¹⁵See Record of Law, 'Deepfakes and the Law: Addressing Legal Accountability for AI-Generated Misinformation' (2025), discussing the Rashmika Mandanna deepfake prosecution (2023, Delhi).

¹⁶IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (10 February 2026), amending r.2(1) of the IT Rules, 2021, inserting cl.(1B)/(zg) [synthetically generated information].

removal of SGI in compliance with the Rules will not itself expose an intermediary to third-party liability under Section 79(2)(a)–(b) of the IT Act.¹⁷

The 2026 Rules are, on their own terms, a significant and overdue regulatory achievement: they finally give Indian law a working definition of synthetic media and impose meaningful, time-bound obligations on the platforms through which deepfakes are overwhelmingly disseminated. Their limitations, for the purposes of this paper, are structural rather than substantive. As delegated legislation made under Section 87(2)(zg) of the IT Act, the 2026 Rules can regulate intermediary due diligence and thereby condition the availability of safe-harbour protection; they cannot create new criminal offences, prescribe punishment for individual creators of deepfakes, or amend the BNS. A person who fabricates and personally circulates a non-commercial but deeply harmful deepfake through private messaging (outside the reach of ‘intermediary’ due-diligence obligations, or below the threshold that triggers platform-level detection) remains subject only to the pre-existing, ill-fitting provisions analysed in Table 1.

3.6 Financial Fraud and the 2026 Judicial Call for Reform

The clearest judicial acknowledgment of this residual gap has come in the context of deepfake-enabled financial fraud, including the phenomenon popularly termed ‘digital arrest’ scams, in which a synthetic video call impersonating a police officer, judge, or senior official is used to coerce victims into transferring funds. Commentary on the Supreme Court’s July 2026 observations records that such conduct continues to be prosecuted only through the general extortion and cheating provisions of the BNS combined with Sections 66C (identity theft) and 66D (cheating by personation) of the IT Act — provisions the Court is reported to have found unsuited to an era of AI-generated synthetic video, particularly given that a defendant may resist forgery-adjacent charges by asserting the deepfake was created for ‘entertainment’ rather than fraudulent purposes, thereby contesting the requisite criminal intent.¹⁸

This is, in the present author’s assessment, the single most important doctrinal signal to emerge from 2026: the apex court itself has identified the absence of an intent standard calibrated to AI-generated content as a live obstacle to effective prosecution, lending institutional weight to the case for legislative reform advanced in Part 5 below.

¹⁷IT Amendment Rules, 2026 (n 24), rr.3(3), 4(4A); see also LiveLaw, ‘Deepfakes, Due Diligence and the Good Samaritan Paradox’ (15 April 2026).

¹⁸TechTimes, ‘India Supreme Court Demands Criminal Law for Digital Arrest, Deepfake Fraud’ (29 July 2026).

3.7 Evidentiary Challenges under the Bharatiya Sakshya Adhiniyam, 2023

A distinct but related problem concerns the authentication of synthetic media as evidence. Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (replacing Section 65B of the erstwhile Evidence Act, 1872) continues to require a certificate authenticating electronic evidence, a regime designed around the integrity of computer-generated records rather than the specific evidentiary problem posed by deepfakes — namely, that the content in question may itself be the forged artefact whose authenticity, rather than mere provenance, is in dispute.¹⁹

Indian courts and forensic laboratories presently lack a statutorily mandated protocol for deepfake detection analogous to the certification regime for ordinary electronic records — there is no requirement that the prosecution adduce forensic AI-detection analysis, no defined chain-of-custody standard for synthetic media exhibits, and no statutory presumption regarding the authenticity (or inauthenticity) of digital content bearing a proper SGI label under the 2026 Rules. This is a significant lacuna: as detection tools and generation tools engage in an escalating technical contest, the reliability of any single forensic method has a shortening shelf life, and the law has yet to prescribe a framework for judicial evaluation of contested authenticity claims.

3.8 Comparative Perspective

The European Union's Artificial Intelligence Act, 2024 adopts a transparency-first model: Article 50 requires deployers of AI systems that generate or manipulate image, audio, or video content constituting a deepfake to disclose that the content has been artificially generated or manipulated, but the AI Act does not itself criminalise deepfake creation — criminal sanction is left to member-state law (for instance, provisions on child sexual abuse material or election-manipulation offences).²⁰

By contrast, several United States states have enacted narrowly tailored criminal statutes: California's Assembly Bill 602 (2019) creates a private civil right of action for non-consensual sexually explicit deepfakes, while Texas and Virginia have criminalised the creation and distribution of deepfakes intended to injure a candidate or influence an election within a specified pre-election window.²¹

¹⁹Bharatiya Sakshya Adhiniyam, 2023, s.63 (certification of electronic evidence); cf. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (on the mandatory nature of the equivalent certificate under s.65B, Evidence Act, 1872).

²⁰Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L 2024/1689, art.50(4).

²¹Cal. Civ. Code § 1708.86 (2019); Tex. Elec. Code § 255.004 (2019); Va. Code Ann. § 18.2-386.2 (2019, as amended).

India’s emerging model — regulatory transparency obligations under the 2026 IT Rules layered atop general-purpose criminal provisions — sits closer to the EU’s disclosure-centred approach than to the US states’ narrowly targeted criminal statutes. The comparative lesson for India is that neither model alone suffices: the EU approach leaves criminal accountability to background law (which, as this paper shows, India’s background law does not adequately supply), while the fragmented US state approach addresses only specific harm categories (election and sexual content) without a generalised offence framework. A comprehensive Indian statute would need to combine EU-style labelling/transparency mandates (already substantially achieved through the 2026 Rules) with a graded, harm-specific criminal offence structure closer to — but broader than — the US state models.

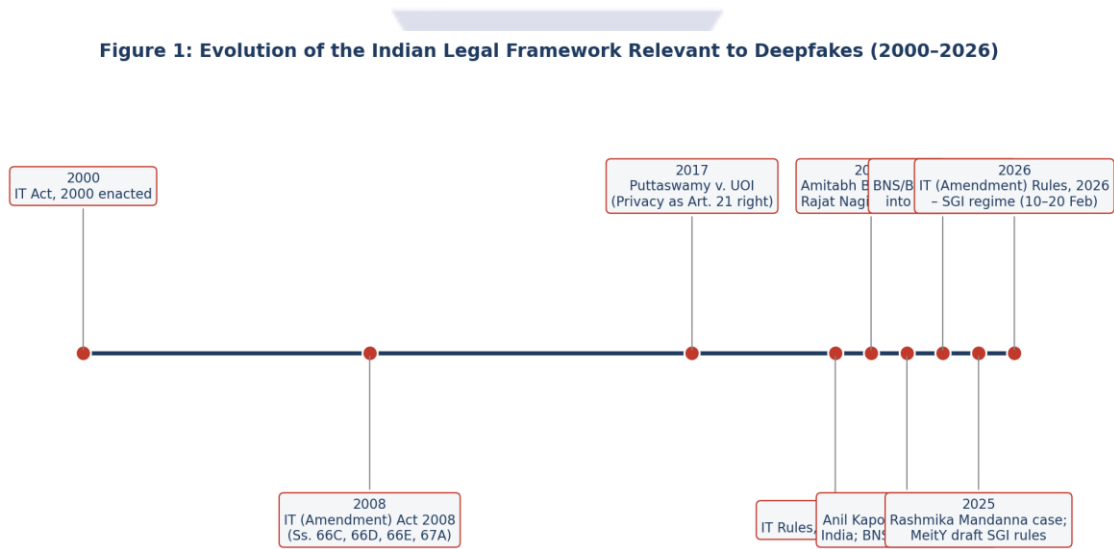


Figure 1: Evolution of the Indian legal framework relevant to deepfakes (2000–2026).

4. FINDINGS

The preceding analysis supports the following findings:

Finding 1: Legislative Definition Arrived Late and Remains Confined to Regulatory (not Criminal) Law

India acquired a statutory definition of synthetic media only in February 2026, through delegated legislation under the IT Act’s intermediary due-diligence framework. No provision of the BNS, 2023 — India’s primary criminal code, in force since July 2024 — references AI-generated or synthetic content, meaning the definitional advance achieved by the 2026 Rules has not been carried through to the substantive criminal law.

Finding 2: Existing Criminal Provisions Require Interpretive Strain

Every provision presently used to prosecute deepfake conduct — Sections 66C, 66D, and 66E of the IT Act; Sections 316–318, 336, 353, and 356 of the BNS — was drafted for a distinct, non-generative harm (credential theft, image capture, documentary forgery, reputational injury caused by true or manipulated-but-not-synthesised statements). Prosecutors and courts have shown considerable interpretive ingenuity (as in the Rashmika Mandanna case), but this ingenuity is itself evidence of a legislative gap rather than a substitute for one.

Finding 3: Civil Personality-Rights Litigation Has Outpaced Criminal Enforcement

Between 2022 and 2026, at least a dozen Indian celebrities have secured sweeping in rem injunctions from the Delhi and Bombay High Courts against deepfake misuse of their persona, compared to a markedly smaller number of reported criminal prosecutions. This asymmetry suggests that well-resourced litigants have found the civil track faster and more reliable than the criminal track — a finding with distributive implications, since non-celebrity victims (particularly women targeted by non-consensual intimate deepfakes) typically lack comparable access to urgent constitutional-court relief.

Finding 4: The 2026 IT Rules Strengthen Platform Accountability but Leave Individual Mens Rea Unaddressed

The tiered takedown timelines, labelling mandates, and Rule 2(1B) safe-harbour clarification meaningfully improve platform-level responsiveness. However, because the Rules operate through intermediary due diligence, they do not and cannot supply a calibrated criminal intent standard for the individual creator of a deepfake — a gap the Supreme Court itself is reported to have flagged in the context of digital-arrest fraud in July 2026.

Finding 5: Evidentiary Authentication Remains an Unaddressed Frontier

The BSA, 2023 retains a certification-based model for electronic evidence inherited from Section 65B of the Evidence Act, 1872, without a specific protocol for authenticating or contesting the authenticity of synthetic media exhibits, leaving trial courts without statutory guidance on forensic AI-detection standards, chain-of-custody for synthetic exhibits, or the evidentiary weight of SGI labelling under the 2026 Rules.

Finding 6: India's Model Diverges from, but Could Learn from, Comparative Approaches

India's emerging framework (labelling/takedown regulation atop general criminal law) mirrors

the EU's transparency-first model but lacks the EU's assumption of robust background criminal law, and has not adopted the US states' technique of narrowly targeted, harm-specific criminal offences (e.g., election-deepfake statutes, statutory civil damages for sexual deepfakes).

5. RECOMMENDATIONS

Based on the findings above, this paper recommends the enactment of a standalone statute — provisionally termed the Digital Impersonation and Synthetic Media (Prevention) Act — built around the following elements:

Recommendation 1: A Statutory, Harm-Graded Deepfake Offence

Parliament should enact a dedicated offence (or a new chapter within the BNS) criminalising the creation or distribution of synthetic media that a reasonable person would mistake for authentic, calibrated by harm category rather than a single undifferentiated offence: (i) non-consensual sexual synthetic media (highest culpability, akin to Sections 67A read with 66E); (ii) synthetic media used for financial fraud or impersonation of public officials (equated with aggravated cheating under the BNS); (iii) synthetic media causing reputational or defamatory harm; and (iv) synthetic political/election content circulated within a defined pre-election window, modelled on the Texas/Virginia approach but adapted to India's Representation of the People Act, 1951 framework.

Recommendation 2: A Calibrated Mens Rea Standard with a Narrow Satire/Parody Defence

The offence should require proof that the accused knew, or had reason to believe, that the synthetic media would be perceived as authentic and would cause the specified category of harm, coupled with an explicit, narrowly drawn defence for clearly labelled satire, parody, and artistic or educational use — directly responding to the Supreme Court's July 2026 concern that an undifferentiated intent standard allows an 'entertainment' defence to defeat legitimate prosecutions, while simultaneously guarding against Article 19(1)(a) overbreadth.

Recommendation 3: Statutory Authentication Protocol under the BSA

The Bharatiya Sakshya Adhiniyam, 2023 should be amended to (a) recognise SGI labelling and provenance metadata under the 2026 IT Rules as admissible, though rebuttable, indicia of authenticity or inauthenticity; (b) mandate forensic AI-detection certification comparable to the existing Section 63 certificate for electronic records; and (c) empower a designated national

forensic authority (building on the existing Indian Computer Emergency Response Team infrastructure) to issue binding technical standards for chain-of-custody in synthetic-media prosecutions.

Recommendation 4: Harmonisation of the 2026 IT Rules with the New Offence

The definition of 'synthetically generated information' in the IT Amendment Rules, 2026 should be adopted verbatim (or by cross-reference) as the definitional basis for the new criminal offence, ensuring that regulatory labelling/takedown obligations and criminal liability operate on a single, consistent definitional foundation rather than the risk of two divergent 'deepfake' definitions developing in parallel.

Recommendation 5: A Victim-Centric, Non-Litigious Compensatory Mechanism

To address the distributive gap identified in Finding 3 — whereby only well-resourced litigants can access civil injunctive relief — the statute should create a summary, low-cost adjudicatory mechanism (for instance, an expanded mandate for the existing Cyber Crime Coordination Centre and State Cyber Cells) empowered to order urgent takedown and modest statutory compensation without requiring the victim to institute a civil suit in a High Court, extending Delhi/Bombay High Court-style protection to non-celebrity victims.

Recommendation 6: Codification of the Personality Right

Rather than leaving the personality right to continued judicial improvisation, Parliament should codify a statutory right of personality (covering name, voice, likeness, and distinctive persona) with express reference to AI-generated infringement, consolidating the Amitabh Bachchan–Anil Kapoor–Jackie Shroff line of cases into predictable statutory text, while preserving the John Doe injunctive mechanism as an interim procedural remedy.

Recommendation 7: Graduated Intermediary Liability Retaining Safe Harbour Incentives

The 2026 Rules' Rule 2(1B) good-samaritan clause should be preserved and extended into the new statute, so that platforms that comply in good faith with detection, labelling, and takedown obligations continue to enjoy safe harbour, while platforms that knowingly host monetised SGI-generation tools without safeguards face a distinct, elevated standard of intermediary liability — addressing the concern (raised in secondary literature) that today's Rules regulate distribution more effectively than they regulate the tools of creation.

6. CONCLUSION

India's legal encounter with deepfakes has proceeded, thus far, in three uneven movements: an early period (2018–2022) in which courts and prosecutors improvised using pre-existing IT Act and Indian Penal Code provisions never designed for generative synthetic media; a middle period (2022–2025) dominated by judicially innovative but access-limited civil personality-rights litigation before the Delhi and Bombay High Courts; and a recent regulatory turn (2026) in which the IT Amendment Rules finally supplied a working definition of synthetically generated information and meaningful platform-level obligations. Each movement has addressed a real and urgent harm, but none, individually or cumulatively, amounts to the comprehensive criminal law framework that the scale and diversity of deepfake-enabled harm in India now demands.

The central argument of this paper is that India does not lack law relevant to deepfakes — it lacks law written with deepfakes specifically in mind. A synthetic voice used to defraud an elderly relative, a synthetic video used to humiliate a private citizen, and a synthetic political speech circulated on the eve of an election are, doctrinally, forced through the same ill-fitting provisions designed respectively for credential theft, unauthorised image capture, and generalised public mischief. The Supreme Court's own reported concern in July 2026 regarding the prosecution of digital-arrest fraud confirms that this is not merely an academic critique but a live obstacle to the effective administration of criminal justice.

This paper has proposed a legislative architecture — a harm-graded, mens rea-calibrated deepfake offence; a statutory evidentiary authentication protocol; harmonisation with the 2026 IT Rules' definitional and labelling regime; a victim-accessible compensatory mechanism; and codification of the judicially developed personality right — designed to consolidate India's fragmented response into a single, constitutionally proportionate statute. Such a framework would not merely close doctrinal gaps; it would shift India's regulatory posture from reactive improvisation, calibrated case by case through celebrity litigation and delegated rule-making, toward a considered, rights-respecting, and genuinely comprehensive response to one of the defining criminal-law challenges of the generative AI era.

REFERENCES

A. Statutes and Delegated Legislation

Constitution of India, 1950, arts.19, 21.

Information Technology Act, 2000 (as amended), ss.66C, 66D, 66E, 67, 67A, 69A, 79.

Indian Penal Code, 1860 (repealed) ss.499–500 (defamation), 463–471 (forgery) [historical reference].

Bharatiya Nyaya Sanhita, 2023, ss.111, 152, 197, 316–318, 336, 353, 356.

Bharatiya Nagarik Suraksha Sanhita, 2023.

Bharatiya Sakshya Adhiniyam, 2023, s.63.

Copyright Act, 1957, ss.38, 38A.

Digital Personal Data Protection Act, 2023.

Representation of the People Act, 1951.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (10 February 2026, effective 20 February 2026).

Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L 2024/1689, art.50.

Cal. Civ. Code § 1708.86 (2019) (United States, California).

Tex. Elec. Code § 255.004 (2019) (United States, Texas).

Va. Code Ann. § 18.2-386.2 (2019, as amended) (United States, Virginia).

B. Cases

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

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

Amitabh Bachchan v Rajat Nagi & Ors, CS(COMM) 819/2022 (Delhi HC, 25 November 2022).

Anil Kapoor v Simply Life India & Ors, CS(COMM) 652/2023 (Delhi HC, 20 September 2023).

Jackie Shroff v The Peppy Store & Ors, CS(COMM) (Delhi HC, 2024).

Karan Johar v Indian Pride Advisory Pvt Ltd & Ors, CS(COMM) (Delhi HC, 19 September 2025).

Aishwarya Rai Bachchan and Abhishek Bachchan personality rights orders (Delhi HC, 2025).

Arijit Singh personality rights order (Bombay HC, 2 August 2024).

Preity Zinta personality rights order (Bombay HC, 2025).

C. Books and Journal Articles

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

Danielle Keats Citron, 'Sexual Privacy' (2019) 128 Yale Law Journal 1870.

Rebecca Delfino, 'Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act' (2019) 88 Fordham Law Review 887.

Lawjournals.org, 'Deepfake Technology and its Criminal Misuse' (2026) 12(2) International Journal of Law.

D. Reports, Advisories and Online Sources

Ministry of Electronics and Information Technology, Government of India, Advisory on Due Diligence to be Observed by Intermediaries (26 December 2023).

Vaish Associates Advocates, 'Regulation of AI-Generated/Deepfake Content and Synthetically Generated Information (SGI) in India – New Rules' (13 February 2026) <www.vaishlaw.com>.

Freshfields Bruckhaus Deringer, 'India Targets Deepfakes and AI-Generated Content: Key Changes under MeitY's 2026 Amendments to the IT Rules' (19 February 2026).

LiveLaw, 'Deepfakes, Due Diligence and the Good Samaritan Paradox; How India's 2026 IT Amendment Rules Resolve Global Platform Liability Debate' (15 April 2026).

Mondaq/Legitpro Law, 'IT Rules 2026 Deepfake Regulation: Three Hour Takedowns and AI Labelling Obligations' (18 March 2026).

Candour Legal, 'AI, Deepfakes, and Personality Rights in India: What Courts Are Doing Without a Statute' (2026).

Naik Naik & Co, 'Delhi HC's Protection to Anil Kapoor; A Landmark Order on Personality Rights' (17 October 2023).

Anantam IAS, 'Delhi High Court Protects Personality Rights, Orders Removal of AI-Generated Fake Content' (2026).

Record of Law, 'Deepfakes and the Law: Addressing Legal Accountability for AI-Generated Misinformation' (2025).

Record of Law, 'Artificial Intelligence and Criminal Liability in India: Addressing the Legal Vacuum in the Era of Deepfakes and Synthetically Generated Information' (2026).

Legal Blur, 'Deepfakes and Indian Law: Copyright & Liability' (2026).

LawArticle, 'Deepfakes in India: Legal Framework and Challenges' (2026).

The Amikus Qriae, 'Deepfake as a Cyber Crime with the Help of AI: Legal Implications and

Need for Reform in India' (2026).

TechTimes, 'India Supreme Court Demands Criminal Law for Digital Arrest, Deepfake Fraud' (29 July 2026).

BananaIP/Intellepedia, 'Safeguarding Digital Identity in the Age of Deepfakes: An Analytical Study of AI Regulation in India with Special Reference to Personality Rights Jurisprudence' (2026).

