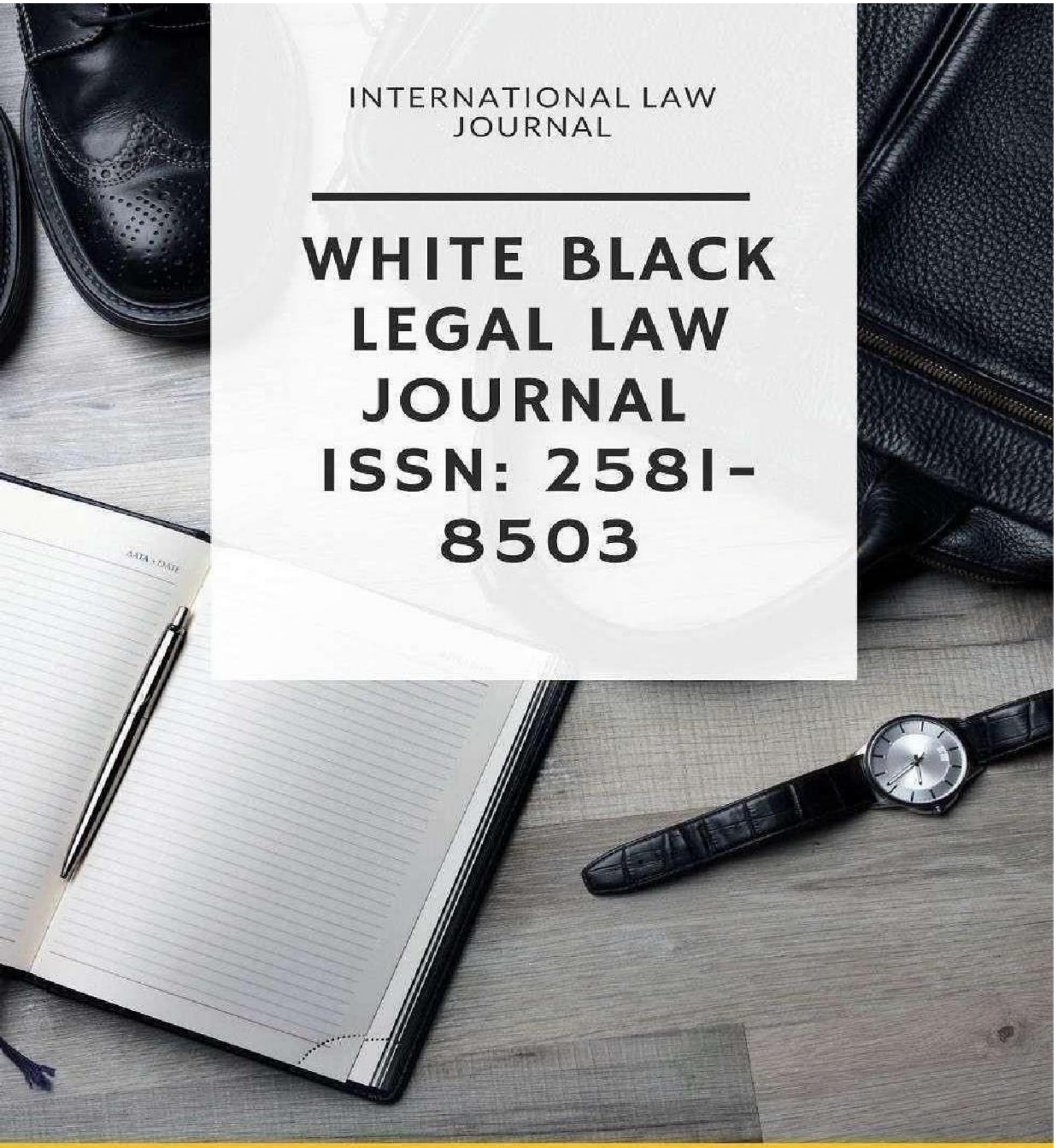

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 7 | June 2026 ISSN: 2581-8503

STOLEN IDENTITIES AND SHALLOW LAWS: A DOCTRINAL AND COMPARATIVE ANALYSIS OF INDIA'S REGULATORY GAP ON DEEPFAKES

AUTHORED BY - RISHISH SINGH & ANIRUDDH SACHIN BAJAJ
1st Year BALLB (Hons.), Gujarat National Law University, Gandhinagar

Abstract

Deepfake technology — synthetic media generated through Generative Adversarial Networks and diffusion models, has moved well beyond novelty. It now enables identity impersonation at scale, producing harms that range from non-consensual intimate imagery to electoral manipulation and financial fraud. India's legal response remains fragmented: three statutes (the IT Act 2000, the BNS 2023, and the DPDP Act 2023) address adjacent harms in partial and overlapping ways, yet not one of them defines deepfake or synthetic media in express terms.[1] Meanwhile, courts have begun constructing a personality rights jurisprudence through cases like *Arijit Singh v. Codible Ventures LLP* (2024), recognising a right to digital persona under Article 21.[2] This paper conducts a doctrinal gap analysis across the three statutes, traces the evolution of identity and personality rights in Indian constitutional law,[3] and examines regulatory models in the United States, United Kingdom, and European Union. Drawing on these strands, it proposes a Synthetic Media Regulation Act for India, a dedicated victim-centred framework built around consent, graduated liability, and platform accountability.

Keywords: *Deepfakes, synthetic media, IT Act 2000, BNS 2023, DPDP Act, personality rights, digital identity, right to privacy, comparative regulation, Synthetic Media Regulation Act.*

[1]See *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248; *Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 SCC 608; *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[2]Information Technology Act, 2000, §§ 66C, 66E, 67, 67A, 69A (India); Bharatiya Nyaya Sanhita, 2023, §§ 296, 318, 319, 351, 356 (India); Digital Personal Data Protection Act, 2023 (India).
[3]*Arijit Singh v. Codible Ventures LLP & Others*, High Court of Bombay, Commercial IP Suit No. 456 of 2024.

I. Introduction

In November 2023, a video circulated across Indian social media showing a prominent Bollywood actress in sexually explicit content she had never participated in. The content was a deepfake, convincing enough to spread rapidly before platforms removed it. The incident was not isolated. In the months around the 2024 general elections, deepfake audio of political leaders was distributed to influence voter sentiment across Uttar Pradesh and Andhra Pradesh. These are not edge cases; they represent the operational reality of a technology that has industrialised identity theft.

Technically, deepfakes are outputs of machine learning architectures, primarily Generative Adversarial Networks (GANs) and, more recently, diffusion models, that synthesise realistic audio, image, or video content by training on data of a target person until the output is indistinguishable from authentic footage. The threshold skill required to produce a convincing deepfake has collapsed over the past five years: what required a research lab in 2018 can now be accomplished through a mobile application in 2026.

India confronts this threat with a legal framework that predates the technology by two decades. The IT Act, 2000 was enacted when social media did not exist. The BNS, 2023, which replaced the Indian Penal Code, carries forward provisions on impersonation, fraud, and obscenity without acknowledging synthetic media. The DPDP Act, 2023 focuses on personal data processing but does not engage with biometric synthesis.[4] Courts have partially filled this vacuum by developing personality rights doctrine, but judicial improvisation cannot substitute for statute when the harms are systematic.

This paper maps the doctrinal gap across India's three primary statutes, traces the jurisprudential evolution of personality rights and digital identity, examines comparative regulatory responses in the US, UK, and EU, and proposes the architecture of a dedicated Indian synthetic media statute. The methodology is doctrinal and comparative: statutes, constitutional provisions, and court judgments are read alongside secondary scholarship to construct an argument for structural reform.

II. The Doctrinal Gap: India's Existing Framework Against Deepfake Harms

The IT Act is India's primary cyber law, amended significantly in 2008. Several provisions have been invoked in deepfake-adjacent cases, but each reveals a structural

[4]Information Technology Act, 2000, § 66C (India). See also Sommya Kashyap, *The Digital Mirage: India's Evolving Legal Battle Against Deepfake Technology*, 22 *SCRIPTed* 162, 175 (2025).

limitation when examined closely. Section 66C criminalises identity theft, targeting the dishonest use of a victim's electronic signature, password, or comparable authentication credential. Prosecutors have argued that deepfakes constitute identity theft since they appropriate a person's facial geometry and voice patterns. The provision, however, was plainly drafted with account credentials and passwords in mind: a deepfake does not use the victim's password, it synthesises their likeness, and the statutory text does not accommodate this distinction.[5]

Section 66E guards bodily privacy by barring the unconsented recording, dissemination, or sharing of intimate images of a person, a provision conceived principally for voyeuristic photography and similar physical intrusions. Courts applying it to deepfake pornography face a definitional obstacle: the intimate imagery in a deepfake is entirely synthetic. No "image of a private area" was ever captured. Section 66E's language requires that something be captured and transmitted, not synthesised from training data.[6] Sections 67 and 67A prohibit publication of obscene and sexually explicit material and do reach deepfake pornography when the output is explicitly sexual, but they are content-type specific. Deepfakes deployed for political disinformation, financial fraud, or reputational harm outside sexual content fall entirely outside these provisions.[7] Section 69A, which empowers the government to block content, has been used reactively, instructing platforms to take down deepfake videos after viral spread. It addresses symptom rather than cause: takedown does not deter creation, punish creators, or compensate victims.[8]

The composite picture from the IT Act is one of provisions designed for analogue-era harms stretched inadequately to cover synthetic media. The Act contains no definition of deepfake, synthetic media, or AI-generated content, imposes no affirmative obligation on platforms to detect or label such content, and provides neither a civil remedy nor a victim compensation mechanism.

When Parliament enacted the BNS to replace the Indian Penal Code, it had the opportunity to include deepfake-specific provisions. It did not. The BNS retains the foundational offences relevant to deepfake misuse: cheating (Section 318), impersonation (Section 319), defamation (Section 356), and criminal intimidation (Section 351), with largely identical language to the IPC.[9] The critical gap is in Section 319 on impersonation, which

[5]Information Technology Act, 2000, § 66E (India).
[6]Id. §§ 67, 67A.
[7]Id. § 69A; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[8]Bharatiya Nyaya Sanhita, 2023, §§ 318, 319, 351, 356 (India).
[9]Id. § 296.

criminalises fraudulently representing oneself as another person. A deepfake creator who generates a video of a politician making a confession does not represent themselves; they represent their technology as producing reality. The mens rea and actus reus elements fit awkwardly. Section 296 extends obscenity provisions in ways potentially applicable to non-consensual deepfake pornography, but the obscenity standard (material that is lascivious and tends to deprave and corrupt) focuses on content effect rather than consent violation. A deepfake deployed for reputational or financial harm outside sexual content causes serious injury without necessarily being obscene. The BNS treats deepfake harms as variants of existing offences rather than a distinct category, missing the technology's essential feature: it weaponises identity itself.[10]

The DPDP Act, when it comes into full operation, will regulate the processing of personal data. Biometric data, including facial geometry, voice patterns, and iris scans, falls within the category whose processing requires explicit consent. Training a deepfake model on images and audio of a real person without their consent is, on a purposive reading, processing their personal data.[11] The limitation is that the DPDP Act's obligations fall on data fiduciaries, meaning organised entities that control how and why personal data is processed. Most deepfake creators are individuals who scrape photographs from social media, not data fiduciaries subject to corporate enforcement architecture. The Act also does not address the output of synthesis: the deepfake video is fabricated data that resembles personal data, not personal data in the traditional sense, and the Act gives no remedy to the person whose likeness was synthesised.[12]

Taken together, the IT Act, BNS, and DPDP Act create a patchwork that misses deepfake harms in three ways. None defines synthetic media or establishes that its non-consensual creation is itself a civil or criminal wrong. None imposes proactive obligations on platforms to detect, label, or remove deepfake content. None provides a victim-centred remedy (compensation, takedown, identity restoration) that matches the actual harm profile. The result is predictable: poor conviction rates, long resolution timelines, and a chilling effect on victims who find the existing system inaccessible.

[10]Digital Personal Data Protection Act, 2023 (India).
[11]Pooja Chopra et al., *Generative AI, Copyright and Personality Rights: A Comparative Legal Perspective*, 6 *Legal Issues in the Digital Age* 23, 31–32 (2025).
[12]*Francis Coralie Mullin v. Administrator, Union Territory of Delhi*, (1981) 1 SCC 608.

III. Personality Rights and the Right to Digital Identity

The right to personality, encompassing control over one's name, likeness, and public persona, does not appear in the Indian Constitution as an express right. Its foundations lie in Article 21. *Francis Coralie Mullin v. Union Territory of Delhi* (1981) read Article 21 as extending to dignified existence, while [13] *Maneka Gandhi v. Union of India* (1978) required that any procedure curtailing personal liberty satisfy standards of fairness, creating constitutional space for rights protecting identity and reputation as dimensions of human dignity.[14]

The pivotal privacy judgment in *K.S. Puttaswamy v. Union of India* (2017) elevated privacy to the status of a fundamental right under Article 21 through a unanimous nine-judge verdict. The bench held that the right's scope reaches informational autonomy, bodily integrity, and personal dignity. Justice D.Y. Chandrachud's concurring opinion further articulated that constitutional protection of personality extends to a person's control over their own narrative and public representation.[15]

Indian courts developed the concept of personality rights through the right of publicity, initially borrowed from American common law. The Madras High Court in *Diljit Dosanjh v. Saregama India Limited* (2023) recognised that a celebrity's voice, name, and likeness constitute protectable personality attributes whose commercial exploitation requires consent. The Delhi High Court in *Amitabh Bachchan v. Rajat Nagi & Others* (2022) issued one of India's first comprehensive personality rights injunctions, protecting the actor's name, voice, image, and personal attributes against unauthorised commercial use across mediums including AI applications.[16]

The case most directly addressing AI-generated synthetic content was *Arijit Singh v. Codible Ventures LLP* (Bombay High Court, 2024). The court restrained the defendants from using AI to clone the singer's voice, generate synthetic performances, or create content that mimicked his artistic identity. The Bombay High Court held that the right to personality includes the right to control digital simulacra of the self, a judicial extension of personality rights specifically to AI-generated outputs, grounded in Article 21, reinforced through Section 38 of the Copyright Act, 1957 and equitable principles of passing off.[17] What *Arijit Singh*

[13] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[14] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[15] *Diljit Dosanjh v. Saregama India Limited*, Madras High Court (2023); *Amitabh Bachchan v. Rajat Nagi & Others*, CS(COMM) 819/2022 (Delhi High Court).
[16] *Arijit Singh v. Codible Ventures LLP & Others*, High Court of Bombay, Commercial IP Suit No. 456 of 2024; Copyright Act, 1957, § 38 (India).
[17] See Shinu Vig, *Regulating Deepfakes: An Indian Perspective*, 17 *J. Strategic Security* 70, 78–80 (2024).

established is the recognition that AI synthesis without consent constitutes a violation of the right to control one's digital persona. A deepfake is not merely a misrepresentation; it is the appropriation of identity, the weaponisation of a person's own features against them.

Indian courts are converging toward recognising a right to digital persona with three components. The right to non-impersonation: no party may simulate a person's identity without consent, whether through classical impersonation or technological synthesis. The right to biometric integrity: a person's facial geometry, voice characteristics, and other biometric attributes deserve protection independent of whether real data was processed. The right to reputational non-falsification: false statements may not be placed in one's mouth or false actions attributed to one's body through technological means. These three components map directly onto the harms deepfakes produce and confirm that the constitutional right to personality is already broad enough to support a statutory framework.[18]

Yet judicial remedies have clear limitations. Injunctions in high-profile celebrity cases require expensive High Court litigation. Most victims cannot access that relief: ordinary individuals targeted by non-consensual deepfake pornography, employees framed in fake confessions, or politicians targeted in disinformation campaigns. Injunctions also operate case-by-case and cannot establish platform-wide obligations, while the deterrence function of civil remedies is weak against anonymous creators operating across jurisdictions. The constitutional jurisprudence provides the normative foundation; statute must supply the scale.

IV. Comparative Regulatory Approaches

The United States has not enacted comprehensive federal deepfake legislation, but the landscape has become considerably more active since 2023. The Defiance Act (2024) broke new ground by establishing a private right of action at the federal level for individuals depicted without consent in intimate synthetic imagery. The No FAKES Act (proposed, 2023–2024) would create a federal right of publicity specifically protecting voice and visual likeness from AI replication without consent. At the state level, California's AB 602 and AB 730 regulate deepfake pornography and electoral deepfakes respectively, while Texas has criminalised deepfakes designed to influence elections.[19][20] The American approach demonstrates two lessons. Fragmentation is a problem: differential state laws create inconsistent protection and are difficult to enforce against cross-state distribution. At the same time, separating harm

[18]Defiance Act, 2024, Pub. L. No. 118-92 (U.S.); No FAKES Act, S. 2770, 118th Cong. (2023–2024).
[19]Cal. A.B. 602 (2019); Cal. A.B. 730 (2019).
[20]Online Safety Act, 2023, c. 50 (U.K.).

categories into discrete statutes allows targeted enforcement and clearer mens rea standards. India, with centralised legislative competence over cyber law, can achieve targeted specificity without the fragmentation problem.

The UK's Online Safety Act, 2023 represents the most comprehensive platform-regulatory response among major democracies. The Act criminalises the distribution of non-consensual intimate deepfake images, imposing liability on both the creator and the platform that fails to act on reports.[21] Critically, it creates a proactive duty on platforms to conduct risk assessments and implement protective systems before harmful content is distributed, not merely after complaints are received.[22] The combination of proactive platform duties, criminal liability for creators and negligent platforms, and victim-centred remedies is the architecture Indian reformers have studied most closely. The limitation from an Indian perspective is its heavy reliance on large platforms self-regulating under statutory duty. India's digital ecosystem is more heterogeneous, with a far larger number of smaller platforms, and platform regulation must be calibrated to this reality.

The EU Artificial Intelligence Act, 2024 classifies deepfakes as high-risk AI applications and imposes mandatory labelling and disclosure requirements. Systems that generate synthetic imagery of real persons must disclose AI generation in a machine-readable format, with express obligations to watermark AI-generated content to allow downstream detection.[23][24] The GDPR provides a parallel data protection remedy: biometric data processing for deepfake creation without consent attracts substantial fines. The EU framework adds a dimension absent from the US and UK approaches: mandatory technical obligation. Platforms and developers must embed disclosure mechanisms, not merely respond to complaints. For India, this offers the clearest template for platform-level technical obligations: the DPDP Act's framework of data fiduciary obligations could be extended to include synthetic media platforms and AI tools, imposing disclosure, watermarking, and detection duties as conditions of operation.

Three lessons emerge from comparative analysis. Dedicated legislation consistently outperforms general law adaptation: jurisdictions with deepfake-specific statutes achieve higher conviction rates and better victim outcomes than those relying on general fraud or

[21]Council Regulation 2024/1689, *Artificial Intelligence Act*, 2024 O.J. (L) 1 (EU).
[22]Shimona Mohan & Sarthak Wadhwa, *Deepfakes and Shallow Laws: Regulating Distorted Narratives in the Political Cyberspace*, 19 *Indian J.L. & Tech.* art. 4 (2024); Devesh Kumar, *Deepfakes, Free Speech, and the Right to Truth*, 6 *Advanced Int'l J. Research* art. AIJFR25041117 (2025).
[23]Online Safety Act, 2023, c. 50, § 179 (U.K.).
[24]Council Regulation 2024/1689, art. 50 (EU) (mandatory disclosure and watermarking for synthetic content depicting real persons).

obscenity provisions.[25] Platform liability must be proactive rather than reactive: notice-and-takedown regimes are structurally inadequate because viral spread of deepfakes happens within hours. Victim remedies must be accessible without High Court litigation: small claims-style administrative tribunals with summary procedures are necessary to make protection available to ordinary citizens.

V. Towards a Synthetic Media Regulation Act for India

A dedicated Synthetic Media Regulation Act (SMRA) for India should rest on four principles grounded in the constitutional and comparative analysis above. **Consent centrality** holds that creating synthetic media depicting an identifiable real person without explicit, informed consent is the foundational civil and criminal wrong; consent must be specific to the type of output and revocable. **Graduated harm-based liability** means criminal and civil liability should scale with harm: creating a deepfake privately differs from distributing it widely, which differs again from deploying it to influence an election. **Proactive platform obligations** require platforms hosting user-generated content to implement deepfake detection systems, label synthetic content, maintain removal registers, and publish transparency reports, tiered by platform size. **Victim-centred remedies** mean criminal conviction should not be the primary remedy; an expedited civil mechanism must be accessible to ordinary people.[26]

A workable statute requires clear definitions the existing framework lacks entirely. The SMRA should define *synthetic media* as audio, video, or image content in which the appearance, voice, words, or actions of an identifiable natural person are generated or substantially fabricated using AI systems, such that a reasonable viewer would believe the content depicts the person's actual conduct. *Non-consensual synthetic media* is synthetic media created or distributed without the explicit, informed consent of the depicted person. *Malicious synthetic media* is non-consensual synthetic media created with the intent to harm the reputation, privacy, financial interests, or democratic participation of the depicted person. These definitions address the core gap: the absence of a legal category that captures the wrongfulness of creating synthetic identity without consent, independent of the ultimate purpose.

On criminal provisions, the SMRA should establish three tiers of liability. Creating or

[25]Ana Zehra & Jyoti Yadav, *Regulation of Deepfakes, Identity Fraud and AI-Created Harms Under New Penal Provisions*, 8 *Int'l J. Multidisciplinary Research* art. IJFMR260273501 (2026); Vishakha Periwal, *Deepfake Laws in India: A Critical Analysis*, 7 *Int'l J. Multidisciplinary Research* art. IJFMR250134563 (2025).
[26]Ganesh Subramanian & Swathi S., *The Legal Dilemma of Deepfakes: AI Liability and the Challenges of Digital Identity Theft*, 6 *Int'l J. Multidisciplinary Research* art. IJFMR240631802 (2024).

distributing non-consensual intimate synthetic media should attract imprisonment of three to seven years, calibrated to Indian sentencing norms. Creating or distributing malicious synthetic media for electoral manipulation, financial fraud, or child sexual exploitation should attract enhanced imprisonment of five to ten years. Operating a platform that knowingly facilitates non-consensual synthetic media after notice and failure to act should attract corporate fines and, for repeated violations, platform suspension.[27] Mens rea requires calibration: for intimate content, intent is presumed from knowledge that the depicted person did not consent; for electoral and financial fraud, specific intent to deceive is required; for platform liability, negligence (failure to act on clear notice) is sufficient.

For civil and administrative relief, a Digital Grievance Adjudicator (DGA), established as a specialist bench of the Information Technology Appellate Tribunal, should have jurisdiction over all civil claims, operating with an online filing system, a 48-hour acknowledgment requirement, power to issue emergency takedown orders ex parte, and a substantive hearing within 30 days. Damages should cover actual loss, non-pecuniary harm, and punitive damages for wilful malice. A victim compensation fund, financed by platform compliance fines, should provide interim compensation while proceedings are pending.[28]

Any effective deepfake statute must also carve out legitimate uses clearly. The SMRA should exempt satire and parody where synthetic media is clearly labelled and no reasonable viewer would mistake it for authentic content; academic and research uses in AI safety and digital forensics; entertainment uses with the depicted person's consent; and historical reconstructions of deceased persons with appropriate labelling. The labelling requirement is non-negotiable: if a satirical deepfake circulates without disclosure, the exemption does not apply.

On intermediary obligations, the SMRA should create a lex specialis for synthetic media requiring: automated deepfake detection on upload for platforms above a user threshold; labelling of detected synthetic media in content metadata; a dedicated in-app reporting mechanism with mandatory 24-hour response; half-yearly transparency reports disclosing removal volumes and detection accuracy; and cooperation with DGA investigations including data preservation. Platforms that comply in good faith should receive safe harbour protection from secondary liability. Platforms that fail to implement required systems or respond to DGA

[27]Zeeshan Shaikh et al., *Exploring Legal and Technical Challenges of Deepfake in India*, 13 *Int'l J. Research Applied Sci. & Eng. Tech.* (2025), https://doi.org/10.22214/ijraset.2025.68385.
[28]Sidharth T. & Guhan T., *Deepfake Technology in Social Media: Social and Legal Implications in India*, 6 *Int'l J. Multidisciplinary Research* art. IJFMR240631284 (2024).

orders should face escalating administrative penalties.[29]

VI. Conclusion

The legal problem with deepfakes in India is not, at its core, a problem of absent values; the constitutional jurisprudence on privacy, dignity, and personality is robust. It is a matter of translation: converting constitutional recognition of the right to digital identity into accessible, scalable, technologically informed statutory protection.

The IT Act's provisions fit deepfake harms poorly because they were written for different harms. The BNS carries forward a century-old vocabulary of fraud and impersonation that does not map onto synthetic identity appropriation. The DPDP Act addresses data processing but not the synthetic output of that processing. Courts have done what they can through personality rights jurisprudence, but injunctions in celebrity cases are not protection for ordinary people.

The comparative evidence is consistent: dedicated synthetic media legislation works better than adapting general law. The UK's proactive platform duties, the EU's transparency and watermarking requirements, and the US's harm-specific civil causes of action each provide architecture that India can adapt. The Indian context adds its own requirements: accessible administrative tribunals, platform obligations calibrated to a heterogeneous ecosystem, and graduated sentencing that reflects scale of harm.

The Synthetic Media Regulation Act proposed here is the statutory translation of rights Indian courts have already recognised, informed by regulatory learning from jurisdictions that have moved faster. The technology will not slow down. Face-swapping that required a GPU cluster in 2018 runs on a mid-range smartphone in 2026. The asymmetry between the ease of creating deepfakes and the difficulty of obtaining legal redress is not a permanent feature of the landscape; it is a legislative choice. The doctrinal foundations are in place. The comparative templates are available. What remains is political will.

[29]Shilpa Agarwal & Vikram Kaushik, *AI-Generated Deepfakes and Political Closures: A Comparative Study of India, UK, and USA (2014–2024)*, *J. Int'l Com. L. & Tech.* (2024).