The Essay Series | *Opinion*

Oxford Law Review, Vol. 1, Issue 1, 2026 DOI: https://10.5281/zenodo.23569663

Deepfakes and the Law in India: Legal Challenges and the Protection Of Digital Identity: An Inquiry into Synthetic Media, Persona Autonomy, and Statutory Integration

Ritika Mishra[1]

© The Author(s), under exclusive licence to Oxford Law Review 2026.

The question of who controls, defines, and protects an individual's digital identity in the era of generative artificial intelligence is not merely a technical query regarding data structures. It is fundamentally an inquiry into power, bodily autonomy, and constitutional freedom: who holds the legal right to harvest a person's biometric traits, what evidentiary threshold must be established before synthetic media is recognized as a civil or criminal violation, and what occurs when an individual's authentic identity is decoupled from their computational likeness? In India, these questions have acquired urgent legal significance as the proliferation of hyper-realistic synthetic media, colloquially termed "deepfakes," intersects with an increasingly formalized system of digital identity and data governance. The underlying conflict is constitutional in nature: can the Indian legal framework safeguard citizens from non-consensual identity manipulation while preserving freedom of expression and technological innovation?

Deepfakes—generated through Generative Adversarial Networks (GANs), autoencoders, and latent diffusion models —represent a paradigm shift in content manipulation. Conventional digital editing involves manual alterations of existing static records. In contrast, deep learning models learn the latent representation of a target's face, voice timbre, and bodily gestures, enabling the algorithmic synthesis of entirely new, highly convincing video or audio sequences that never occurred in physical reality. By separating human agency from visual and vocal representation, synthetic media weaponizes identity. In India, this technological disruption exposes significant vulnerabilities across constitutional rights under Articles 14, 15, 19(1)(a), and 21, as well as statutory doctrines within criminal law, intellectual property, and civil remedies.

Building expertise in deepfake law requires navigating the structural gap between static legal provisions and fluid algorithmic capabilities. Indian jurisprudence has historically addressed identity theft through property-based torts, passing off, or specific penal codes aimed at

[1] **Chandigarh Law College, CGC University, Mohali, Punjab, India;** ✉ **ritikamishra1504@gmail.com**

Copyright © Oxford Law Review. (www.oxfordlr.com)

Oxford Law Review, Vol. 1, Issue 1, 2026 DOI: https://10.5281/zenodo.23569663

impersonation. However, deepfakes generate harms that do not fit neatly into these classical silos. Non-consensual synthetic sexually explicit media (NCSEM), financial extortion using voice cloning, political disinformation, and the systemic erosion of digital evidence represent distinct harms requiring distinct analytical frameworks.

Constitutional recognition does not automatically give practical freedom. A person may have a right in principle to identity protection while facing procedural and evidentiary steps that make it hard to enforce that right. The difference between the existence of a right and the administrative conditions needed to use that right is essential to understand digital persona protection in India. If identity recognition relies on algorithmic verification, police certification, or platform discretion, the State and private entities become the real gatekeepers of a right that the Constitution originally framed as an intrinsic personal freedom.

This tension can be seen through the link between identity and administrative clarity. Modern digital governance relies on structured data, biometric registries, and standard verification procedures to provide public benefits, run databases, and manage identity systems. James C. Scott in *Seeing Like a State* explains how administrative structures manage societies by simplifying social realities into standardized categories. While this simplification aids administrative efficiency, it can also erase nuanced personal realities that do not fit official frameworks.

In the context of generative AI, digital identity governance faces a parallel issue. Digital identity is experienced personally, culturally, and socially. In India, personal identity incorporates name, likeness, vocal cadence, reputation, and bodily integrity. A legal framework that assumes static models of identity risks making protection depend on whether a citizen's compromised identity fits existing legal definitions under legacy statutes. When the law fails to keep pace with synthetic replication, individual autonomy is subordinated to institutional gaps.

The constitutional basis for regulating deepfakes and protecting the digital persona stems directly from the Supreme Court of India's landmark jurisprudence on autonomy, dignity, and self-determination. In *National Legal Services Authority v Union of India* (NALSA), the Supreme Court affirmed that self-defined identity is an integral component of personal autonomy and dignity under Article 21 of the Constitution. The Court held that self-determination of identity forms the core of personal liberty, while Articles 14, 15, and 19(1)(a) inform the broader constitutional protection of personhood. While NALSA examined gender identity, its foundational constitutional principle applies equally to digital persona: an individual's identity belongs intrinsically to the person, free from unauthorized appropriation or forced alteration by external actors.

This framework was expanded in *Justice K S Puttaswamy (Retd) v Union of India*, where a nine-judge bench unanimously recognized privacy as a fundamental right grounded in dignity, autonomy, and personal liberty under Article 21. The Court explicitly recognized "informational privacy" and "spatial privacy" as key facets of this right, establishing that individuals must retain control over the collection, processing, and dissemination of personal data, including biometric features. Justice Kaul's concurring opinion specifically highlighted the risks of ubiquitous computing, algorithmic profiling, and unauthorized data harvesting, emphasizing that dignity is compromised when personal data is processed without consent.

Copyright © Oxford Law Review. (www.oxfordlr.com)

Oxford Law Review, Vol. 1, Issue 1, 2026 DOI: https://10.5281/zenodo.23569663

Applying the *Puttaswamy* framework to generative AI demonstrates that unauthorized deepfake generation inflicts a direct constitutional injury. When an individual's biometric features—facial vectors, voice recordings, physical movements—are scraped to train generative models or create synthetic depictions, two distinct constitutional violations occur. First, the non-consensual processing of biometric features violates informational self-determination under Article 21. Second, placing an individual in a synthetic scenario—whether sexually explicit, defamatory, or deceptive—violates personal dignity and moral integrity.

Furthermore, in *Navtej Singh Johar v Union of India*, the Supreme Court emphasized that individual autonomy, equality, and dignity protect citizens from discriminatory or abusive actions. Although *Navtej Singh Johar* addressed Section 377 of the Indian Penal Code, its core constitutional reasoning establishes that social prejudice or technological capability cannot undermine fundamental rights, and that fundamental freedoms cannot depend on majority approval or technical convenience.

A. Freedom of Expression and Synthetic Speech

Conversely, generative AI tools are also utilized for creative expression, political satire, artistic performances, and educational recreations, engaging Article 19(1)(a) of the Constitution. The Supreme Court's decision in *Navtej Singh Johar* affirmed that expressive freedom is central to democratic discourse. Consequently, legal measures targeting deepfakes cannot take the form of blanket prohibitions or overbroad restrictions on generative software code.

Any statutory or judicial restriction on synthetic media must satisfy the strict proportionality test articulated in *Puttaswamy*: it must be backed by a clear law, serve a legitimate State aim, demonstrate a rational connection to that aim, represent the least restrictive measure available, and maintain a balance between individual rights and public interest. Regulating deepfakes requires distinguishing between malicious identity theft and legitimate artistic or political expression.

In the absence of explicit, dedicated legislation governing synthetic media, Indian High Courts have relied on common law remedies, passing off, and the constitutional right to privacy to shield individual identity from AI-driven exploitation. This judicial expansion has been driven by litigation involving public figures seeking to prevent unauthorized commercial exploitation of their likeness and voice.

The foundational common law basis for identity protection was recognized in *Titan Industries Ltd v Ramkumar Jewellers*, where the Delhi High Court held that an individual possesses an exclusive right to control the commercial use of their identity. The Court observed that publicity rights stem from the right to privacy and protect against unauthorized commercial appropriation. However, classical publicity rights were developed around static print and broadcast media.
Generative AI required a major expansion of this doctrine to address synthetic clones.

A. The Anil Kapoor Framework for Synthetic Persona

Copyright © Oxford Law Review. (www.oxfordlr.com)

Oxford Law Review, Vol. 1, Issue 1, 2026 DOI: https://10.5281/zenodo.23569663

In *Anil Kapoor v Simply Life India & Ors* (2023), the Delhi High Court directly confronted the threat posed by generative AI platforms, deepfake tools, and voice cloning software. The plaintiff, a prominent actor, sought injunctive relief against multiple entities using AI to generate synthetic videos, voice recordings, and commercial merchandise using his likeness, signature catchphrases, and mannerisms without authorization.

Granting an omnibus ex-parte injunction, the High Court held that while freedom of expression permits fair comment, parody, and satire, it does not allow the commercial exploitation of an individual's persona using generative AI. The Court recognized that voice, image, name, and vocal mannerisms constitute fundamental attributes of personal identity protected under the right to privacy and personality rights. Crucially, the Court directed platform providers and domain registrars to immediately disable access to links containing synthetic content, establishing a clear judicial precedent for fast interim relief in deepfake disputes.

B. Vocal Timbre Protection: The Arijit Singh Precedent

This protection was extended by the Bombay High Court in *Arijit Singh v Codible Ventures LLP & Ors* (2024). The suit targeted AI platforms that allowed users to convert singing voices into the plaintiff's distinctive vocal timbre, as well as platforms using his name and likeness to train AI models. The Bombay High Court affirmed that an individual's voice is an intrinsic component of identity. Training an AI model on an artist's audio recordings to generate new synthetic recordings without consent was held to violate personality rights and Article 21 privacy protections.

Despite judicial developments in personality rights, India's statutory framework remains fragmented across multiple enactments drafted before generative AI. Prosecutors, litigants, and courts must combine provisions from cyber law, criminal codes, data protection, and copyright law to address synthetic media harms.

A. The Information Technology Act, 2000 & Intermediary Rules

The Information Technology Act, 2000 (IT Act) contains several provisions applicable to deepfakes. Section 66D penalizes cheating by personation using a computer resource with imprisonment up to three years. Section 66E addresses privacy violations by penalizing the intentional capturing or publishing of private area images without consent. Sections 67 and 67A penalize transmitting obscene or sexually explicit material in electronic form.

The primary regulatory enforcement mechanism operates through Section 79 of the IT Act, which grants safe harbor immunity to intermediaries, conditional upon exercising due diligence. Under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (amended in 2022 and 2023), intermediaries must inform users not to host or upload content that impersonates others or depicts non-consensual sexually explicit material. Under Rule 3(1)(b), intermediaries must remove or disable access to non-consensual explicit or artificially altered impersonation content within twenty-four hours of receiving a complaint.

Copyright © Oxford Law Review. (www.oxfordlr.com)

Oxford Law Review, Vol. 1, Issue 1, 2026 DOI: https://10.5281/zenodo.23569663

B. Criminal Law Integration: Bharatiya Nyaya Sanhita, 2023 (BNS)

The replacement of the Indian Penal Code, 1860 by the Bharatiya Nyaya Sanhita, 2023 (BNS) updated provisions relevant to synthetic media. Section 318(4) of the BNS penalizes cheating by personation, covering instances where deepfakes are used to deceive victims for financial gain or impersonate officials. Section 336(4) addresses forging electronic records, prosecuting individuals who create false electronic records to cause injury.

Additionally, Section 78 of the BNS penalizes stalking, including electronic monitoring, while Section 79 penalizes acts intended to insult the modesty of a woman, encompassing non-consensual synthetic explicit imagery. Criminal defamation under Section 356 of the BNS remains available where synthetic media damages reputation.

C. Digital Personal Data Protection Act, 2023 (DPDP)

The Digital Personal Data Protection Act, 2023 (DPDP Act) creates a statutory regime for processing digital personal data. Under Section 4, personal data may only be processed for a lawful purpose with consent or for specified legitimate uses. Because facial vectors, voice patterns, and biometric traits constitute personal data, harvesting such data to train generative AI models or create synthetic media requires explicit consent under Section 6.

Section 8 mandates that Data Fiduciaries ensure the accuracy and completeness of personal data used to make decisions affecting individuals or disclosed to other Data Fiduciaries. Processing inaccurate synthetic data that attributes false actions to a person violates this obligation. Additionally, the DPDP Act empowers the Data Protection Board of India to impose penalties up to two hundred and fifty crore rupees for failing to implement reasonable security safeguards under Section 33.

D. Copyright Act, 1957 & Performers' Rights

The Copyright Act, 1957 provides protections that intersect with voice cloning and synthetic performance. Section 38 grants performers a "performer's right" lasting fifty years. Section 38A gives performers the exclusive right to make sound or visual recordings of their performance and communicate them to the public.

Section 38B enshrines performers' moral rights, granting the right to be identified and to restrain or claim damages for distortion, mutilation, or modification prejudicial to reputation. Where an AI model ingests an artist's recorded performance to synthesize a new performance without consent, it distorts artistic integrity, engaging Section 38B moral rights.

Generative AI destabilizes digital evidence principles in court proceedings. Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA)—which replaces Section 65B of the Indian Evidence Act, 1872—electronic records require a mandatory certificate for admissibility. The Supreme Court in

Copyright © Oxford Law Review. (www.oxfordlr.com)

Oxford Law Review, Vol. 1, Issue 1, 2026 DOI: https://10.5281/zenodo.23569663

Anvar P V v P K Basheer held that electronic records without proper certification are strictly inadmissible, a position reaffirmed in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal.*

However, Section 63 of the BSA was designed to verify the operational integrity of the device that stored or printed the electronic file. A Section 63 certificate confirms that the computer system operated properly; it does not verify whether the content within the file was generated by an algorithmic model. A perfectly certified electronic file can contain a synthesized deepfake. Formal device certification cannot detect internal algorithmic manipulation.

This limitation generates the "Liar's Dividend," wherein authentic video or audio evidence presented in court is discredited by parties claiming it is an AI-generated deepfake. When public and judicial confidence in visual evidence declines, the probative value of uncorroborated electronic records diminishes. Courts must move beyond standard Section 63 certificates and incorporate cryptographic provenance standards, reverse image analysis, and expert forensic testimony under Section 39 of the BSA.

Developing deep legal insights requires identifying structural misalignments between legal doctrines and technological realities. Several counterintuitive patterns govern the deepfake ecosystem in India:

A. Misclassification of NCSEM as Defamation

A common legal error in handling non-consensual sexually explicit deepfakes is framing complaints primarily as criminal defamation under Section 356 of the BNS. Defamation protects public reputation—an external social asset. In contrast, non-consensual sexual depiction inflicts psychological harm, violates bodily privacy, and degrades dignity under Article 21. Framing the harm as defamation allows defendants to raise statutory defenses such as truth or public interest, which are inapplicable to synthetic sexual media. Complaints should center on bodily integrity, privacy, and sexual modesty under Sections 78 and 79 of the BNS and Section 67A of the IT Act.

B. The Publicly Available Data Exemption Loophole in DPDP 2023

Section 3(c)(ii) of the DPDP Act, 2023 exempts personal data "made publicly available by the Data Principal" from consent mandates. This creates a major regulatory blind spot. When citizens post photos or audio online, a literal interpretation suggests AI developers may scrape these files without consent to train generative models. Courts must interpret "publicly available" restrictively, distinguishing between data shared for social interaction and data harvested for AI model training.

C. The Open-Source Enforcement Paradox

Regulatory mandates requiring AI platforms to embed watermarks or content filters are effective against centralized commercial providers. However, malicious actors predominantly utilize open-source diffusion models hosted locally offline. Because open-source software can be modified to strip watermarks and content filters, statutory mandates targeting platform intermediaries fail to

Copyright © Oxford Law Review. (www.oxfordlr.com)

Oxford Law Review, Vol. 1, Issue 1, 2026 DOI: https://10.5281/zenodo.23569663

deter sophisticated bad actors. Regulation must combine platform oversight with hardware-level digital signatures embedded directly into camera sensors and microprocessors at capture time.

To transition from a reactive statutory posture to a rights-protective framework, India requires a coherent regulatory strategy:

1. *Sui Generis Digital Persona Legislation:* India should enact specialized legislation establishing a statutory "Right to Digital Identity Integrity," defining unauthorized biometric extraction, voice cloning, and synthetic likeness creation as distinct civil wrongs and strict-liability offenses when conducted without explicit consent.
2. *Unbundled Digital Consent Architecture:* Giving consent to publish an image or audio file must not imply consent for AI feature extraction or model fine-tuning. Legally binding consent for generative AI must be explicit, granular, and revocable.
3. *Presumption Framework under BSA Section 63:* The BSA should incorporate a statutory presumption framework. Where prima facie evidence shows an electronic record lacks cryptographic provenance metadata or contains synthetic artifacts, the burden of establishing authenticity should shift to the party submitting the record.
4. *Restructuring Intermediary Accountability:* Section 79 safe harbor under the IT Act should be conditioned on intermediaries deploying automated provenance detection and providing fast, transparent appeal mechanisms for victims of non-consensual synthetic media.

The challenge of deepfakes and synthetic media in India represents a pivotal moment for technology law and constitutional jurisprudence. The issue extends beyond technical detection or incremental amendments to cybercrime statutes. It touches the core of constitutional governance: whether the legal system can maintain human dignity, individual agency, and epistemic truth in a digital ecosystem where perception can be computationally manipulated.

As demonstrated by Supreme Court jurisprudence in *NALSA*, *Puttaswamy*, and *Navtej Singh Johar*, Indian constitutionalism centers on personal autonomy, dignity, and protection from arbitrary state or private interference. High Courts have operationalized these principles in *Anil Kapoor* and *Arijit Singh*, establishing that voice, likeness, and persona constitute intrinsic attributes of human identity that cannot be converted into unconstrained data for commercial or malicious exploitation.

Moving forward, addressing the deepfake challenge requires a balanced approach. Overbroad legislation risks chilling creative expression, political satire, and legitimate AI research protected under Article 19(1)(a). Conversely, statutory passivity leaves citizens vulnerable to severe violations of bodily integrity, financial security, and privacy under Article 21. By establishing a dedicated statutory framework for digital persona integrity, resolving evidentiary paradoxes under Section 63 of the BSA, closing data scraping exemptions under the DPDP Act, and mandating technical provenance standards, India can build a legal framework that preserves truth, protects personal identity.

References

National Legal Services Authority v Union of India (2014) 5 SCC 438, AIR 2014 SC 1863.

Copyright © Oxford Law Review. (www.oxfordlr.com)

Oxford Law Review, Vol. 1, Issue 1, 2026 DOI: https://10.5281/zenodo.23569663

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

Navtej Singh Johar v Union of India (2018) 1 SCC 791.

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

Arijit Singh v Codible Ventures LLP & Ors CS(COMM) 891/2024 (Bom HC, 26 July 2024).

Titan Industries Ltd v Ramkumar Jewellers (2012) 50 PTC 486 (Del).

Anvar P V v P K Basheer (2014) 10 SCC 473.

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

Constitution of India, arts 14, 15, 19(1)(a), 21.

Information Technology Act, 2000 & IT Intermediary Rules, 2021.

Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

Copyright Act, 1957 (Act 14 of 1957).

Publisher's Note

Oxford Law Review maintains neutrality with respect to the opinions, interpretations, and conclusions expressed in published articles, as well as jurisdictional claims in published maps and institutional affiliations. The views and arguments presented in this article are solely those of the author(s) and do not necessarily reflect the views of Oxford Law Review, its editors, or its publisher. Responsibility for the accuracy, originality, and integrity of the content rests with the author(s). Publication of an article does not constitute an endorsement by Oxford Law Review of the views expressed therein. All rights relating to the article are governed by the applicable publishing agreement between the author(s) or other rightsholder(s) and the publisher, together with applicable law.

Copyright © Oxford Law Review. (www.oxfordlr.com)