



DEEP FAKES AND DIGITAL PERSONHOOD: A CONSTITUTIONAL FRAMEWORK FOR IDENTITY PROTECTION IN THE AGE OF GENERATIVE AI

Teena Lalchandbhai Taviyad

ABSTRACT

The rapid proliferation of generative artificial intelligence and synthetic media has shifted legal challenges from informational data privacy to identity manipulation. Traditional legal frameworks predominantly treat digital impersonation through financial fraud or defamation lenses, leaving a critical vacuum in addressing non-economic harms caused by deepfakes. This research paper evaluates the constitutional and statutory necessity of safeguarding “digital personhood”—the unique, intangible representation of an individual in the virtual sphere. Adopting a doctrinal and analytical qualitative legal methodology, the study analyzes the constitutional guarantees under Article 21 of the Indian Constitution, asserting that the right to dignity and personal liberty must encompass a fundamental “Right to Digital Bodily Integrity.” Furthermore, the paper critiques the statutory limitations within the newly enacted Bharatiya Nyaya Sanhita (BNS), 2023, the Digital Personal Data Protection (DPDP) Act, 2023, and highlights the evidentiary challenges presented by Section 61 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023. The findings demonstrate that ad-hoc judicial remedies remain insufficient for ordinary citizens. Consequently, the paper recommends a comprehensive framework featuring statutory recognition of digital personhood, compulsory cryptographic AI watermarking, and standardized forensic verification protocols to protect human dignity in the generative AI era.

KEYWORDS: Generative AI, Deepfakes, Digital Personhood, Article 21, BNSS 2023, Identity Protection

LL.B, LL.M, UGC NET

How to Cite:

Teena Lalchandbhai Taviyad (2026), Deep fakes and Digital Personhood: A Constitutional Framework for Identity Protection in the Age of Generative AI, International Educational Journal of Science & Engineering (IEJSE), Vol: 9, Issue: 9, 01-05

1. INTRODUCTION

The rapid proliferation of generative artificial intelligence (AI) has fundamental implications for the legal understanding of human identity. Earlier digital rights discourses focused primarily on informational privacy—protecting personal data against unauthorized collection or dissemination. However, the advent of sophisticated deep learning architectures, such as Generative Adversarial Networks (GANs), has shifted the paradigm from data protection to complete identity manipulation. Generative AI tools can now fabricate hyper-realistic audio, video, and imagery that clone an individual’s likeness, voice, and demeanor with astonishing accuracy.

This technological leap introduces the concept of synthetic media, where a person’s physical and vocal identity can be detached from their agency and deployed without consent. As algorithmic capabilities outpace statutory adaptation, the legal challenge is no longer confined to controlling data flows. Instead, it centers on safeguarding “digital personhood”—the unique, intangible representation of an individual in the virtual sphere.

2 STATEMENT OF PROBLEM

Traditional Indian legal mechanisms remain structurally ill-equipped to address the nuanced harms inflicted by deepfakes. Existing laws overwhelmingly categorize identity misuse through

restricted legal frameworks: financial fraud, property theft, or classical defamation. While these statutory remedies address tangible economic loss or external reputational damage, they fail to grasp the core harm of synthetic media—the violation of individual self-determination.

Deepfake creation directly attacks an individual's digital bodily integrity, personality rights, and moral autonomy. By forcing a person to implicitly perform acts, express views, or appear in contexts they never chose, generative media disrupts the core guarantees of human dignity protected under Article 21 of the Constitution of India. Furthermore, current statutes—including the Information Technology Act, 2000 and updated criminal provisions under the Bharatiya Nyaya Sanhita (BNS), 2023—rely on reactive frameworks designed for static digital impersonation rather than dynamic, AI-driven identity fabrication. This statutory vacuum creates a severe constitutional challenge, leaving citizens without robust legal safeguards to defend their digital likeness against algorithmic appropriation.

3. REVIEW OF LITERATURE

The legal discourse surrounding synthetic media has rapidly evolved from general concerns of cyber fraud to complex questions of constitutional identity. A review of contemporary Indian legal scholarship reveals three major thematic clusters:

(A). Evolution from Privacy to Digital Personhood

Early scholarship centered primarily on data protection following the landmark Puttaswamy judgment. However, recent legal literature highlights that informational privacy alone is insufficient to address generative AI. Scholars argue that deepfakes do not merely leak data; they hijack human representation, necessitating the legal recognition of “digital bodily integrity” as an extension of personal liberty under Article 21.

(B). Inadequacy of Existing Criminal & IT Statutes

Literature analyzing the Information Technology Act, 2000 and the newly enacted Bharatiya Nyaya Sanhita (BNS), 2023 indicates a regulatory void. While provisions like Section 66D of the IT Act and Section 318 of BNS address cheating by personation, researchers emphasize that these statutes require intent to defraud or cause financial

loss. They fail to capture non-economic harms such as non-consensual deepfake pornography or political identity manipulation.

(C). Evidentiary and Regulatory Hurdles

Recent studies on electronic evidence under Section 61 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 stress the growing “epistemic crisis” in Indian courts. Authors note that traditional standards for authenticating digital records are ill-equipped for hyper-realistic synthetic media, creating severe challenges for both prosecution and defense in establishing truth. Furthermore, analysis of the Digital Personal Data Protection (DPDP) Act, 2023 reveals that while it regulates personal data processing, it lacks direct, proactive mechanisms to compel AI platforms to watermark or prevent synthetic identity creation.

4. OBJECTIVES OF THE STUDY

The primary objective of this study is to examine the constitutional and statutory dimensions of synthetic media, specifically deepfakes, and to propose a legal framework for protecting digital personhood in India. The specific objectives are:

- To analyze the legal shift from informational privacy to digital personhood in the context of generative AI and synthetic media.
- To examine the scope of Articles 14, 19, and 21 of the Constitution of India in protecting individual dignity, bodily integrity, and moral autonomy against deepfake manipulation.
- To assess the adequacy and limitations of the Bharatiya Nyaya Sanhita (BNS), 2023 and the Information Technology Act, 2000 in penalizing non-consensual synthetic impersonation.
- To evaluate the evidentiary challenges under Section 61 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 and the regulatory scope of the Digital Personal Data Protection (DPDP) Act, 2023 regarding generative AI.
- To formulate concrete, constitutional-compliant legal reforms for safeguarding digital identity in India.

5. RESEARCH QUESTIONS

To achieve the aforementioned objectives, this research paper addresses the following key questions:

1. How does generative AI transform the legal

understanding of human identity, and why is informational privacy inadequate to protect against deepfake misrepresentation?

2. Does the fundamental right to life and personal liberty under Article 21 encompass a “Right to Digital Bodily Integrity” and protection against unauthorized synthetic cloning?
3. To what extent do the penal provisions under the Bharatiya Nyaya Sanhita (BNS), 2023 fall short in addressing non-economic and non-consensual deepfake harms?
4. How can Indian courts navigate the authenticity and admissibility standards for electronic evidence under Section 61 of the BNSS, 2023 in the presence of hyper-realistic synthetic media?

6. RESEARCH METHODOLOGY

This study adopts a doctrinal, qualitative, and analytical research methodology. The research relies on both primary and secondary open-access legal sources:

- **Primary Sources:** The Constitution of India; contemporary legislations including the Bharatiya Nyaya Sanhita (BNS), 2023, the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, the Information Technology Act, 2000, and the Digital Personal Data Protection (DPDP) Act, 2023; alongside landmark judicial pronouncements of the Supreme Court of India.
- **Secondary Sources:** Open-access legal research papers, law review articles, reports of parliamentary committees, and authoritative academic commentaries on constitutional law, cyber law, and artificial intelligence ethics.

The analytical framework combines constitutional interpretation with critical legislative analysis to evaluate statutory gaps and suggest normative solutions.

7. SUBSTANTIVE ANALYSIS

(A) Constitutional Foundations of Digital Personhood under Article 21

The emergence of generative AI demands an expansion of constitutional jurisprudence. Traditionally, Article 21 has evolved dynamically to encompass rights unimagined by the framers of the Constitution—ranging from bodily autonomy to environmental protection. In the landmark Puttaswamy judgment, the Supreme Court recognized privacy not merely as

secrecy, but as spatial, informational, and decisional autonomy.

However, deepfakes present a challenge distinct from data privacy breaches. While informational privacy concerns the unauthorized disclosure of truthful facts, synthetic media involves the deliberate fabrication of a false human persona. When an individual’s likeness, voice, or facial features are weaponized to create hyper-realistic deepfakes, the violation transcends data theft—it strikes at the core of human dignity and self-determination.

Digital personhood represents the legal projection of individual identity into the virtual sphere. Just as physical bodily integrity protects an individual from unconsented physical touching, “digital bodily integrity” must protect against unconsented virtual cloning. Forcing an individual to implicitly perform actions, express political views, or participate in non-consensual sexual acts through synthetic media directly violates their moral agency under Article 21. True personal liberty cannot exist if individuals lose control over how their physical and vocal identities are presented to the world.

(B) The Interplay between Article 19 Freedom and Personality Rights

The proliferation of deepfakes also complicates the constitutional balance between freedom of expression under Article 19(1)(a) and individual identity rights. Generative AI tools are frequently deployed under the guise of parody, satire, artistic creation, or political commentary. While genuine satire enjoys constitutional protection, synthetic identity theft often crosses into manipulative misrepresentation.

Indian jurisprudence has recognized personality rights primarily for public figures to prevent commercial exploitation of their likeness. However, in the era of generative AI, personality rights must be democratized. Non-consensual deepfakes—whether targeting public figures or ordinary citizens—exceed the reasonable restrictions permissible under Article 19(2). When synthetic content is used to defame, harass, or mislead the public, the constitutional shield of free speech cannot protect the creator at the expense of another’s fundamental right to dignity and identity protection.

(C) Statutory Deficits in Penal and Data Legislation

India's existing penal framework demonstrates significant structural gaps when confronted with AI-generated synthetic media:

1. Gaps in Bharatiya Nyaya Sanhita (BNS), 2023:

Section 318 of the BNS penalizes "cheating by personation." However, this offense traditionally requires proof of fraudulent intent to cause financial loss or gain. Deepfakes generated for non-economic harms—such as revenge pornography, emotional distress, or political character assassination—do not neatly fit within this pecuniary threshold. Similarly, while Section 356 penalizes defamation, standard civil and criminal defamation remedies remain reactive, slow, and inadequate to halt the viral spread of synthetic media.

2. Deficits in Information Technology Act, 2000:

Sections 66C and 66D of the IT Act address identity theft and impersonation using computer resources. Designed in the era of static web technologies, these provisions assume a human actor stealing credentials or using static photos. They do not account for autonomous AI algorithms capable of generating original, synthetic personas in real time.

3. Limitations of DPDP Act, 2023:

The Digital Personal Data Protection Act, 2023 regulates the processing of personal data by Data Fiduciaries. While biometrics and facial features constitute personal data, the DPDP Act primarily focuses on lawful processing and consent architecture. It lacks proactive statutory mandates for AI developers—such as compulsory cryptographic watermarking, algorithmic provenance tracking, or immediate algorithmic takedown duties for synthetic identity clones.

(D) Evidentiary Challenges under Section 61 of BNSS, 2023

The criminal justice system relies heavily on the authenticity of electronic records. With the implementation of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, Section 61 governs the admissibility and proof of electronic evidence.

Generative AI introduces a severe "epistemic crisis" into judicial proceedings. Historically, courts operated under the presumption that video and

audio recordings provided reliable, objective proof of real-world events. Advanced deepfakes shatter this presumption. Under Section 61, proving the chain of custody and integrity of electronic records becomes extraordinarily complex when hyper-realistic synthetic media can be created using widely accessible software.

Without standardized forensic verification protocols, courts face a dual risk:

- Fabricated synthetic evidence may be wrongly admitted, leading to miscarriages of justice.
- Authentic digital evidence may be routinely dismissed by defense counsel invoking the "liar's dividend"—claiming that real audio or video evidence is merely a deepfake.

8. FINDINGS

The primary findings of this research paper demonstrate that generative AI fundamentally alters the relationship between law and human identity:

1. Inadequacy of Privacy Architecture:

Current fundamental rights jurisprudence focuses heavily on informational privacy. Deepfakes do not merely leak confidential information; they hijack human agency and force an individual to visually or vocally perform unconsented acts. This creates a distinct legal injury that requires the judicial recognition of a "Right to Digital Bodily Integrity" under Article 21.

2. Statutory Gaps in Penal Law:

The Bharatiya Nyaya Sanhita (BNS), 2023 focuses primarily on pecuniary fraud or reputational harm in its cheating and impersonation provisions (Sections 318 and 356). Consequently, non-economic deepfake violations—such as non-consensual synthetic media or political misrepresentation—lack direct criminal remedies.

3. Procedural Vulnerability under BNSS, 2023:

Section 61 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 relies on traditional chain-of-custody assumptions for electronic records. Without statutory mandates for forensic verification, courts risk either accepting manipulated media or falsely rejecting legitimate digital evidence due to the "liar's dividend."

4. Regulatory Incompleteness of DPDP Act, 2023:

The Digital Personal Data Protection Act regulates data processing and consent, but it lacks proactive technical obligations for AI developers—such as compulsory cryptographic watermarking or provenance tracking at the model level.

5. Ad-Hoc Judicial Remedies:

While the High Courts have increasingly stepped in to protect individual identity and publicity attributes against AI misuse, current relief relies almost entirely on civil single-judge interim injunctions. This fragmented legal protection leaves ordinary citizens without clear, accessible statutory remedies.

9. SUGGESTIONS

To bridge the gap between AI capabilities and constitutional protections, the following reforms are recommended:

1. Statutory Recognition of Digital Personhood:

Enact a dedicated legal framework—or amend the BNS, 2023—to explicitly criminalize unauthorized synthetic identity creation, treating non-consensual digital cloning as a direct offense against personal autonomy and dignity.

2. Mandatory AI Watermarking and Provenance:

Require AI developers and platform intermediaries to embed immutable, cryptographic digital watermarks and metadata provenance into all generative AI outputs.

3. Standardized Forensic Protocols Under BNSS:

Establish specialized forensic validation guidelines under Section 61 of the BNSS, 2023 to assist judicial officers in verifying electronic records and evaluating deepfake evidence.

4. Expedited Digital Takedown Architecture:

Empower an administrative or statutory authority to mandate the rapid removal and hashing of non-consensual deepfakes across intermediary platforms within strict timeframes.

10. CONCLUSION

Generative AI presents an existential challenge to the classical understanding of human identity and legal evidence. As synthetic media blurs the boundaries of physical reality, the legal system can no longer view identity theft solely through the lens of financial fraud or property rights.

Protecting individual identity in the digital age requires a constitutional evolution—one that expands Article 21 to safeguard “digital personhood” and moral agency against algorithmic appropriation. By combining proactive statutory regulations, robust evidentiary verification under the BNSS, 2023, and technical accountability from AI platforms, India can establish a balanced framework that fosters technological innovation while steadfastly preserving human dignity.

REFERENCES

1. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
2. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
3. Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
4. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).
5. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
6. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
7. Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts*, HarperCollins India (2019).
8. Upendra Baxi, *Human Rights in a Post-Human World: Critical Essays*, Oxford University Press (2009).
9. Deepa Varadarajan, *A Personality Right for the Digital Age*, 82 Geo. Wash. L. Rev. 1471 (2014).
10. Anil Kapoor v. Simply Life India & Ors., 2023 SCC OnLine Del 6914.
11. Jaikishan Kakubhai Saraf v. The Peppy Store & Ors., 2024 SCC OnLine Del 3664.
12. Ananth Padmanabhan, *Digital Evidence in the Age of Synthetic Media*, 15 Nat'l L. Sch. India Rev. 88 (2022).