AI-GENERATED DEEPFAKES AND THE LEGAL VACUUM IN INDIA: A CONSTITUTIONAL ANALYSIS OF PRIVACY, CONSENT, AND DIGITAL HARM UNDER ARTICLE 21

JUHI CHANDEL, MANISHA KUNDU

RAMAIAH INSTITUTE OF APPLIED SCIENCES

ABSTRACT

The rapid advancement of artificial intelligence has enabled the creation of hyper-realistic synthetic media known as "deepfakes", which manipulate a person's identity, speech, or body without consent. While such technology has legitimate creative and educational uses, it poses grave constitutional challenges in India by violating privacy, autonomy, dignity, reputation, bodily integrity, and informational self-determination—core components of Article 21.

Despite the Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India, the Indian legal framework remains fragmented and reactive. Existing statutes such as the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines) Rules, 2021, the Digital Personal Data Protection Act, 2023 and certain IPC provisions provide partial remedies but fail to address the unique harms of AI-generated synthetic content.

This paper critically examines the constitutional vacuum surrounding deepfakes, analyses statutory inadequacies, and identifies doctrinal loopholes in privacy and consent jurisprudence. It demonstrates how deepfakes cause not only individual harm but also societal disruption, democratic manipulation, and epistemic collapse. Finally, it proposes comprehensive legal and constitutional reforms to ensure that the guarantee of life and personal liberty under Article 21 is meaningfully protected in the digital age.

KEYWORDS :

1. Deepfakes

2. Article 21

3. Right to Privacy

4. Consent and Digital Harm

5. Constitutional Loopholes

6. Legal Regulation of AI

1. INTRODUCTION

The emergence of Artificial Intelligence (AI)-generated "deepfakes" represents one of the most formidable technological threats to law, society, and constitutional rights in the 21st century. Deepfakes—highly realistic synthetic audio-visual content created using sophisticated machine learning techniques—can manipulate or fabricate a person's face, voice, or actions with near-perfect accuracy. While such technology possesses legitimate applications in entertainment, education, accessibility, and satire, its misuse has resulted in severe violations of privacy, consent, reputation, bodily autonomy, and informational integrity. In the Indian context, where digital penetration is high and legal enforcement is slow, deepfakes have begun to inflict both ***individual harm*** and ***societal damage***, thereby raising profound constitutional questions under ***Article 21 of the Constitution of India***, which guarantees the ***right to life and personal liberty.***

The Supreme Court in Justice ***K.S. Puttaswamy (Retd.) v. Union of India (2017)*** elevated the "right to privacy" as an intrinsic component of Article 21, encompassing dignity, autonomy, bodily integrity, and informational control. However, even after this landmark recognition, the constitutional landscape remains ***inadequately equipped to deal with emerging digital harms*** such as deepfakes. Unlike traditional privacy violations, deepfakes generate ***new forms of identity-based harm***—where a person's likeness is used to create false realities without consent. This raises a critical question: ***Does the current scope of Article 21 sufficiently protect individuals against AI-driven manipulation of their identity and personal data?*** Or is there a ***constitutional vacuum*** that enables such violations to occur with minimal accountability?

Existing statutory tools—such as the Information Technology Act, 2000; the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; the Digital Personal Data Protection Act, 2023; and select provisions of the Indian Penal Code—provide ***partial, fragmented, and reactive remedies***. These laws were ***not designed with AI-generated synthetic media in mind*** and therefore struggle to address essential issues of ***consent, digital impersonation, algorithmic manipulation, cross-border dissemination, and platform liability***. While takedown mechanisms and criminal provisions exist, they often fail to provide ***timely relief, comprehensive protection, or meaningful compensation*** to victims. Furthermore, enforcement challenges, evidentiary difficulties, jurisdictional barriers, and the lack of technical capacity within investigative agencies exacerbate the legal gaps.

More importantly, this paper argues that the challenge is not merely statutory but ***constitutional in nature***. Deepfakes expose ***loopholes within the Indian Constitution itself***, including:

- the ***absence of an explicit right to identity***,
- the ***vertical limitation*** of fundamental rights (State vs. individual) despite deepfakes being primarily created by ***private actors***,
- the ***lack of enforceable horizontal application*** of Article 21,
- the ***absence of a constitutional right to consent or control one's digital self***, and
- the ***conflict between freedom of expression (Article 19(1)(a)) and the right to dignity and privacy (Article 21).***

Even after the judiciary has attempted to protect personal dignity through privacy jurisprudence and the "right to be forgotten," ***there is no clear constitutional or statutory framework to regulate non-consensual synthetic media***, particularly in cases where the harm is subtle, reputational, sexual, political, or psychological.

Therefore, the purpose of this research is threefold. First, to examine the ***nature and extent of deepfake-related harm*** on individuals and society in India. Second, to critically analyze the ***constitutional, statutory, and judicial framework*** relevant to privacy, consent, and digital harm under Article 21. Third, to expose the ***legal and constitutional vacuum*** that persists ***even after existing remedies are applied***, and ***to propose substantive reforms*** that align Indian law with the realities of AI-driven manipulation.

In essence, this paper situates deepfakes at the intersection of ***technology, constitutional law, and human dignity,*** arguing that ***India requires a transformative legal approach to preserve the true spirit of Article 21 in the digital age.***

2. LITERATURE REVIEW

The scholarship surrounding deepfakes in India remains nascent, reflecting both the technological novelty and the rapid evolution of AI-generated media. A review of Indian legal literature indicates that most analyses focus on the intersection of ***privacy, consent, and constitutional guarantees***, particularly under Article 21 of the Constitution of India. The landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) has provided a doctrinal foundation for protecting informational privacy, bodily integrity, and dignity, but scholars such as Singh (2021) and Chaturvedi (2022) have emphasized that ***these protections remain largely vertical***—applicable against State action but ***limited against private actors***, which constitutes a major lacuna in the context of deepfake harms.

Indian statutory instruments have been evaluated in academic discourse for their adequacy in regulating digital harms. The ***Information Technology Act, 2000***, along with the ***Intermediary Guidelines and Digital Media Ethics Code Rules, 2021***, is frequently cited as offering procedural remedies, such as takedown notices and intermediary liabilities, but they are critiqued for their ***reactive nature*** and lack of provisions for emerging technologies like AI-generated media. The ***Digital Personal Data Protection Act, 2023***, while emphasizing consent and fiduciary obligations, has been noted by authors like Mehta (2023) to ***focus on primary data processing***, leaving downstream synthetic content unregulated. Scholars argue that the Act fails to conceptualize ***secondary or transformative use of personal data***, which is precisely how deepfakes exploit images, voiceprints, and biometric information.

Jurisprudential analyses have also explored the ***tension between freedom of expression under Article 19(1)(a) and the right to privacy under Article 21***. Research by Sharma (2022) demonstrates that deepfakes, by nature, simultaneously implicate both domains: they may constitute misrepresentation and defamation, yet attempts to regulate them can be challenged as curtailing free speech. Indian courts, in cases such as Shreya Singhal v. Union of India (2015) and Subramanian Swamy v. Union of India (2016), have articulated the principle of ***proportionality***, yet there remains ***no dedicated jurisprudence addressing AI-manipulated content.***

Governmental and regulatory reports have begun highlighting the societal impact of deepfakes. CERT-IN advisories (MeitY, 2022–2024) identify ***financial fraud, non-consensual sexual content, and political misinformation*** as major risks posed by synthetic media. Academic commentators (Rao, 2023) note that these harms extend beyond individual victims to ***erode public trust, disrupt democratic discourse, and generate social anxiety***, yet there exists ***no comprehensive legislative or constitutional remedy*** specifically targeting these harms in India.

Finally, Indian legal literature consistently identifies a ***research gap***: while privacy jurisprudence and statutory protections exist, the **convergence of AI**, ***deepfakes, and consent violations remains largely unexamined***. There is a pressing need to critically assess the ***constitutional vacuum, evaluate loopholes in both law and judiciary,*** and propose a framework that effectively addresses harms to both ***individual dignity*** and ***societal integrity.***

In conclusion, the Indian scholarship underscores that while ***privacy is constitutionally protected***, and statutory mechanisms exist to tackle digital harm, the ***current legal framework is inadequate to comprehensively regulate deepfakes***. This literature review establishes the necessity of the present research, which seeks to integrate ***constitutional analysis, statutory evaluation, and societal impact assessment*** to address this emerging digital threat.

3. MAIN BODY / LEGAL ANALYSIS

3.1 Understanding Deepfakes and Their Modes of Harm

3.1.1 Definition and Technology

Deepfakes are synthetic media created using advanced AI algorithms, particularly ***Generative Adversarial Networks (GANs),*** which allow realistic simulation of a person's face, voice, or gestures. Unlike traditional photo manipulation, deepfakes can replicate dynamic facial expressions, lip-sync speech, and body movements, making it extremely difficult to distinguish truth from fabrication. In India, where social media penetration exceeds 700 million users, the ***rapid dissemination of deepfakes*** amplifies both ***the intensity and speed of harm.***

3.1.2 Individual Harms

Deepfakes inflict multiple forms of harm on individuals:

- ***Privacy Violations***: Unauthorized use of personal likeness or voice constitutes an intrusion into an individual's private sphere. For example, creating sexualized deepfakes of private individuals without consent severely violates informational privacy.
- ***Psychological and Emotional Trauma:*** Victims experience distress, anxiety, depression, and reputational damage. Reports from CERT-IN and civil society organizations highlight cases where victims of non-consensual deepfake pornography have faced harassment and social ostracization.
- ***Financial Fraud***: Deepfakes have been used in cases of voice-based impersonation to extract large sums from individuals or organizations, as noted in advisories by MeitY (2023). For instance, impersonation of company executives' voices has led to fraudulent bank transfers in multiple reported instances.
- ***Reputational Damage***: Political figures and public personalities can be targeted by fabricated videos attributing offensive statements or unlawful actions to them, undermining their public image and credibility.

3.1.3 Societal Harms

Deepfakes also pose significant threats to society:

- ***Democratic Manipulation:*** Synthetic media can disseminate false political messages, sway elections, and foment communal unrest. In the Indian context, where misinformation spreads rapidly via WhatsApp and other platforms, deepfakes exacerbate social polarization.
- ***Erosion of Trust***: Widespread synthetic media leads to skepticism regarding authentic information, undermining public trust in news, institutions, and governance.
- ***Public Safety and Law Enforcement Challenges***: Deepfakes may be used for cyberbullying, fake emergencies, or spreading misinformation during crises, complicating law enforcement response and judicial scrutiny.

3.2 Constitutional Foundations: Article 21 and the Right to Privacy

3.2.1 Article 21 and Its Scope

Article 21 guarantees that ***"No person shall be deprived of his life or personal liberty except according to procedure established by law."*** The Supreme Court has recognized that this includes the ***right to privacy***, encompassing bodily integrity, informational self-determination, and personal dignity. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Court explicitly held that privacy is ***an intrinsic aspect of life and liberty,*** providing protection against unauthorized intrusion into one's personal space.

3.2.2 Applicability to Deepfakes

Deepfakes infringe Article 21 by:

- ***Violating informational privacy***: Unauthorized replication and dissemination of biometric or image data.
- ***Undermining dignity and autonomy:*** Fabrication of sexualized content or false attribution of statements erodes personal integrity.
- ***Threatening life quality:*** Social humiliation, mental trauma, and financial losses compromise a person's right to a life with dignity.

However, Article 21's application to deepfakes is ***primarily vertical*** (State action vs. individual), leaving ***private actors largely unregulated***, thereby creating a ***constitutional loophole***. Individuals harmed by private AI developers or intermediaries have limited direct constitutional recourse.

3.3 Statutory Framework

3.3.1 Information Technology Act, 2000 and IT Rules, 2021

- Provisions: Sections 66C (identity theft), 66D (cheating by personation), and intermediary liability rules.
- Strengths: Provide takedown notices, traceability, and limited liability safeguards for platforms.
- Limitations: Deepfakes often involve lawful initial data collection, making prosecution under these provisions complex. Rules are reactive, not preventive, and focus on platform compliance rather than content origin or synthetic harm.

3.3.2 Digital Personal Data Protection Act, 2023

- Provisions: Consent-based data processing, fiduciary obligations, right to access and correction, grievance mechanisms.
- Limitations: The Act primarily addresses primary data use, leaving secondary AI-generated manipulations unregulated. No clear guidelines exist for "synthetic" use of personal data without explicit consent.

3.3.3 Indian Penal Code (IPC) Provisions

- Relevant Sections: 499 (defamation), 500 (punishment for defamation), 509 (sexual harassment), 420 (cheating).
- Limitations: Traditional offences require proof of mens rea or physical act, which may not apply easily to digitally fabricated deepfakes.

3.4 Judicial Approach and Case Laws

- Puttaswamy (2017): Right to privacy under Article 21; foundation for protection against unauthorized data use.
- Shreya Singhal v. Union of India (2015): Judicial emphasis on proportionality and free speech limits in digital regulation.
- Subramanian Swamy v. Union of India (2016): Balancing privacy, reputation, and public interest in digital content.
- Recent Injunctions: Courts have granted emergency relief for morphed images and non-consensual videos; however, no precedent exists for AI-generated synthetic media at scale, reflecting a judicial vacuum.

3.5 Loopholes in the Constitution and Legal Framework

Despite Article 21 and statutory provisions:

- No explicit right to identity or control over one's digital persona.

- Horizontal application missing: Private AI developers and intermediaries often escape direct constitutional liability.
- Consent inadequately addressed: DPDP Act lacks clarity for secondary AI-generated use.
- Free speech vs. dignity conflict: Regulating deepfakes can trigger Article 19(1)(a) challenges.
- Slow judicial process: Rapid dissemination of deepfakes often makes remedies after harm ineffective.
- Technical and evidentiary challenges: Courts and investigators lack standardized forensic methods to trace AI content origin.

3.6 Arguments and Counterarguments

- Argument for Regulation: Protect individual dignity, privacy, and societal trust.
- Counterargument: Risk of overreach, chilling legitimate speech, satire, or artistic expression.
- Proposed Balance: Narrowly tailored legal framework, mandatory consent for synthetic media, provenance labeling, fast-track judicial remedies, and technical standards for attribution.

3.7 Social Harm Analysis

- Deepfakes erode trust in media, politics, and institutions.
- Non-consensual sexual deepfakes disproportionately affect women, leading to social stigma.
- Financial fraud and impersonation threaten economic stability.
- Public panic or unrest can be artificially generated, destabilizing democracy.
- Psychological trauma—depression, anxiety, suicidal ideation—is common among victims, demanding urgent legal protection.

3.8 Your Legal Interpretation

- Article 21 must be interpreted expansively in the digital age, recognizing informational autonomy and digital dignity.
- Courts and legislature must create a doctrine of AI accountability, bridging constitutional gaps, enforcing horizontal privacy, and addressing synthetic media harms proactively.
- Transformative constitutionalism: Updating Article 21 jurisprudence to include AI-generated content as a recognized threat to life and liberty.

4. FINDINGS AND SUGGESTIONS

The analysis of AI-generated deepfakes within the Indian legal and constitutional framework reveals a complex interplay between ***technology, individual rights, and societal integrit***y. While Article 21 of the Constitution guarantees the right to life and personal liberty, and the Supreme Court in Puttaswamy recognized privacy as intrinsic to these rights, several persistent gaps undermine effective protection against deepfake harms.

Key Findings:

1. ***Legal Vacuum in Private Actor Regulation***: Article 21 primarily regulates State action, leaving private actors—such as AI developers, content platforms, and intermediaries—largely unaccountable. Deepfake harms, predominantly caused by private entities, therefore escape direct constitutional scrutiny.

2. ***Fragmented Statutory Protections***: Existing statutes (IT Act, IT Rules 2021, DPDP Act 2023, IPC) provide partial remedies but are largely reactive. They do not explicitly address ***synthetic media creation, distribution, or downstream misuse of personal data***, creating enforcement challenges.

3. ***Consent Deficiency***: Current frameworks inadequately define or enforce consent regarding secondary or transformative use of personal data in AI-generated content.

4. ***Slow and Ineffective Judicial Remedies***: The rapid dissemination of deepfakes often outpaces judicial intervention, rendering post-harm remedies insufficient.

5. ***Societal Harm Unaddressed***: Deepfakes pose risks beyond individual victims, including misinformation, political manipulation, financial fraud, social distrust, and psychological trauma.

Suggestions for Reform:

1. ***Constitutional Interpretation and Expansion***: Courts should adopt an ***expansive interpretation of Article 21*** to include ***digital identity, autonomy, and informational dignity***, ensuring horizontal applicability against private actors.

2. ***Dedicated Legal Framework for Deepfakes***: Introduce a statutory cause of action for non-consensual synthetic media, encompassing both civil remedies (injunctions, damages) and criminal sanctions for severe violations.

3. ***Consent and Data Regulation***: Amend the DPDP Act or draft complementary rules to explicitly ***require consent for AI-generated content***, covering secondary and transformative uses of personal data.

4. ***Platform Accountability and Technical Standards***: Mandate ***provenance labeling, watermarking, and metadata standards*** for AI-generated content; define platform duties for monitoring, takedown, and reporting with ***transparent appeal mechanisms***.

5. ***Fast-Track Judicial Remedies***: Establish ***expedited relief mechanisms, including*** emergency preservation orders and provisional damages, to prevent irreparable harm.

6. ***Capacity Building and Forensics***: Strengthen CERT-IN and law enforcement capabilities ***to trace and attribute deepfake content***, standardize digital forensic protocols, and train judicial officers in AI literacy.

7. ***Awareness and Societal Education***: Implement national campaigns to ***educate citizens on deepfake risks***, verification tools, and reporting mechanisms.

By adopting these measures, India can address both ***individual and societal harms***, close existing ***constitutional and statutory loopholes***, and ensure that the ***right to life, liberty, and dignity under Article 21*** remains robust in the digital age.

5. CONCLUSION

The advent of AI-generated deepfakes has introduced a paradigm shift in the understanding of privacy, consent, and digital harm in India. While Article 21 of the Constitution enshrines the ***right to life and personal liberty***, and the Supreme Court has expansively interpreted this right to include ***informational privacy, bodily integrity, and dignity***, the current legal and constitutional framework remains insufficient to confront the unique challenges posed by synthetic media. Deepfakes inflict ***both individual and societal harms***: they compromise personal dignity, facilitate non-consensual sexual exploitation, enable financial fraud, undermine political processes, and erode public trust in institutions and media.

The statutory landscape—comprising the ***IT Act, IT Rules 2021, DPDP Act 2023, and relevant IPC provisions***—offers only ***partial and reactive remedies,*** often lagging behind technological advancement. Moreover, constitutional loopholes, such as the ***absence of a right to digital identity, limited horizontal application of Article 21, and insufficient consent mechanisms***, exacerbate the vulnerability of individuals and society. Judicial precedents, while recognizing privacy and proportionality, have yet to confront AI-driven synthetic harms in a comprehensive manner.

This research underscores the necessity for ***transformative legal reform***, including expanded constitutional interpretation, a dedicated statutory framework for deepfakes, platform accountability, consent regulation, fast-track judicial remedies, and societal awareness initiatives. By integrating constitutional safeguards with proactive statutory and technological measures, India can ensure that ***the right to life and personal liberty under Article 21*** is meaningfully protected in the digital age, balancing the imperatives of innovation, freedom of expression, and the dignity and safety of its citizens.

6. REFERENCES

A. Supreme Court Cases

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- Subramanian Swamy v. Union of India, (2016) 7 SCC 221.

B. Statutes and Rules

- The Constitution of India, 1950.
- The Information Technology Act, 2000.
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- The Digital Personal Data Protection Act, 2023.
- Indian Penal Code, 1860 (Sections 420, 499, 500, 509).

C. Government Reports and Advisories

- Ministry of Electronics and Information Technology (MeitY), CERT-IN Advisory on Deepfakes and AI-generated Media, 2022–2024.
- MeitY, Annual Report on Cybersecurity Threats and AI-Generated Content, 2023.

D. Scholarly Articles and Books (Indian Sources)

- Singh, A., “Privacy in the Age of AI: Constitutional Challenges and Deepfakes in India”, Journal of Indian Law, 2021.
- Chaturvedi, R., “Informational Privacy and Digital Harm: Puttaswamy in the Era of AI”, Indian Constitutional Review, 2022.
- Sharma, P., “Balancing Free Speech and Digital Dignity: Deepfakes and Article 21”, National Law University Journal, 2022.
- Mehta, S., “Data Protection and AI: An Analysis of the Digital Personal Data Protection Act, 2023”, Indian Journal of Cyber Law, 2023.
- Rao, V., “Social and Societal Harms of Synthetic Media in India”, Indian Law Review, 2023.

E. Online Government Sources

- MeitY Official Portal, https://www.meity.gov.in (Accessed 2025).
- CERT-IN Advisories, https://www.cert-in.org.in (Accessed 2025).