International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Deepfake Technology and Consent: The Need for Stronger Cyber Laws in India

Saanya Sachdeva[a]

[a]Gitarattan International Business School, GGSIPU, Delhi, India

Received 11 May 2026; Accepted 10 June 2026; Published 13 June 2026

The traditional digital adage, 'seeing is believing,' has become increasingly irrelevant today. With the rise of artificial intelligence, it has become remarkably simple to manipulate audio or video content. As a result, recordings that were once relied upon in courtrooms to verify authenticity and as primary evidence can no longer be fully trusted. This article examines the rise of synthetically generated information (SGI) and its impact on digital consent and individual autonomy. In response to this, the Ministry of Electronics and Information Technology has introduced various amendments, mandating that platforms take reasonable measures to identify synthetically generated content, and has reduced content takedown timelines. An analysis of the IT Act of 2000 and Bhartiya Nyaya Sanhita, 2023, shows that India still lacks specific legislation on deepfakes, highlighting clear gaps in how Indian law protects a person's digital identity. This article highlights the need for a clearer legal framework focused on protecting digital bodily autonomy. This could help protect individuals from AI-related harms.

Keywords: *SGI, BNS, deepfake technology, digital consent.*

INTRODUCTION

The rapid advancement of AI has widened the gap between technological innovation and existing legal frameworks. For decades, audio and visual media were used to verify facts and truth in legal and historical contexts. In the court of law, audio and visual evidence were considered reliable, but with the emergence of technology, their authenticity can no longer be assumed automatically. With advanced machine learning models like Generative Adversarial Networks, malicious actors can now easily clone someone's voice, facial expressions, and physical movements.[1]

When emerging technologies such as AI-generated synthetic media undermine the authenticity of digital records, they severely weaken India's fundamental constitutional values. Under Article 21 of the Constitution of India, the Supreme Court has established that privacy is a fundamental right. It is an essential aspect of human dignity.[2]

Deepfake technology directly threatens privacy and sovereignty, detaching an individual's persona from their physical self without consent. This technological mismatch creates a significant challenge because India's current laws are not equipped to handle such advanced technology. The constitutional vulnerability highlights a void in India's legal and regulatory framework. The Information Technology Act includes provisions governing identity theft and cheating, but it remains fundamentally insufficient to address the sophisticated challenges of AI.[3]

This Article will also examine the constitutional dimensions of digital bodily autonomy. As bodily autonomy increasingly intersects with digital identity, concerns regarding personal digital identity have become more significant in the digital age.[4]

Although the newly launched Bhartiya Nyaya Sahita provides a strong deterrence, it still lacks specific provisions regulating Artificial Intelligence. The article will explore the

[1] Ian Goodfellow et al., 'Generative Adversarial Networks' in *NIPS'14: Proceedings of the 28th International Conference on Neural Information Processing Systems - Volume 2* (MIT Press 2014)
[2] *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[3] Information Technology Act 2000, ss 66C – 66E
[4] Rajat Khosla et al., 'Sexual and reproductive health and rights and bodily autonomy in a digital world' (2023) 31(4) Sex Reprod Health Matters <https://pmc.ncbi.nlm.nih.gov/articles/PMC10629411/> accessed 08 May 2026

multidimensional threat of deepfakes, processes of financial fraud and ultimately propose comprehensive legislative recommendations, advocating for the urgent enactment of a standalone Deepfake Regulation Act.

HOW DEEPFAKE TECHNOLOGY WORKS AND THE THREAT TO DIGITAL CONSENT

Let's begin with a question: why do we need stronger cyber laws? To get the answer, first, we need to understand the technical mechanisms that make deepfake technology a serious threat to human autonomy. Historically, a human editor was required to manipulate the video or audio recording, and in modern times, that human element has been replaced by artificial intelligence. At the core of the synthetic media is a sophisticated class of artificial intelligence known as Generative Adversarial Networks.[5] To see why India needs stronger cyber laws, get into the details of Generative Adversarial Networks. Instead of spending hours editing a video, this system sets up a competitive process between two digital entities: a Generator and a Discriminator.[6]

The generator is the part of the AI software that creates the deepfake. Its only job is to create something from the very beginning. The Discriminator is the part that does not create anything. Its only use case is to check whether the work done by the generator looks real or fake. It catches mistakes in the work. This automated system of a generator and a discriminator directly undermines personal autonomy and limits consent. This reduction of human identity to an unauthorised digital consent collides with the provisions of Article 21 of the Indian Constitution that guarantees dignity and privacy.[7]

DOES THE USE OF DEEPFAKES VIOLATE ARTICLE 21?

The misuse of deepfake technology not only leads to cybercrime but also hinders the fundamental right of Article 21 of the Indian Constitution.[8] By deploying automated software to

[5] Ian Goodfellow et al., 'Generative Adversarial Networks' (2014) arXiv:1406.2661 <https://arxiv.org/abs/1406.2661> accessed 08 May 2026
[6] Robert Chesney and Danielle Citron, 'Deepfakes and the New Disinformation War ' (*Foreign Affairs*, 11 December 2018) <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> accessed 08 May 2026
[7] *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[8] Constitution of India 1950, art 21

replicate a person's physical features and voice without their knowledge, this leads to technological exploitation of the person; it's like using resources without consent. Now let's dive into the two domains, right to privacy and bodily autonomy.

The Infringement on the Right to Privacy: According to the landmark case of KS Puttaswamy v Union of India, a nine-judge bench decided to establish that privacy is an inseparable part of the right to life under Article 21, shielding both information and decisional choices.[9] Consequently, creating deepfakes takes away a person's power to manage their own public image. It turns someone's unique identity into an unauthorised digital product. The harm goes much deeper than just data theft; it completely captures a person's life and leaves them completely vulnerable online. When the technology can make someone look or perform the way they never did, this shows that control is destroyed. This makes the promises of Article 21 empty.

The Violation of Bodily Autonomy and Integrity: In the past, the law usually protected the body from actual touching or being locked up. Nowadays, the courts recognise that your body is your own absolute space.[10] With the deepfakes, the attacks are not just physical but also damage personal control over oneself, which is just as painful. The issue becomes incredibly dangerous when deepfakes are used to make non- consensual videos or fake photos. The Supreme Court of India has made it clear that having control over the body is a vital part of human dignity under Article 21.[11] When the software changes a person's feature without permission, it takes away their basic right of consent. It treats their identity like a cheap object to look at. In the end, the real damage is not the constitutional damage, but the direct attack on a person's mental health and personal autonomy.

HOW CURRENT INDIAN LAWS FALL SHORT?

To deal with the issues caused by deepfakes, Indian courts and lawyers usually rely on a mix of traditional criminal laws and information technology rules. These laws are made to regulate the digital world, but some specifications are missing related to the non-consensual deepfakes.

The Information Technology Act 2000: The IT Act is our main weapon against cybercrime, but it only protects at the surface level when it comes to deepfakes. For instance, section 66E

[9] *Justice K S Puttaswamy (Retd) and Anr v Union of India and Ors* (2017) 10 SCC 1
[10] *Suchita Srivastava and Anr v Chandigarh Administration* (2009) 9 SCC 1
[11] *Navtej Singh Johar and Ors v Union of India Th Secretary Ministry of Law and Justice* (2018) 10 SCC 1

punishes people violating privacy and take or share images of someone's private parts without permission.[12]

This works fine with explicit deepfakes, but it is completely useless if a deepfake puts a victim's face on full clothed body to ruin their reputation or spread political statements. Similarly, Sections 67 and 67A punish sharing obscene and explicit material online.[13] However, relying on these sections creates a common conceptual problem. They treat the issue as a crime against public morality rather than a violation of individual rights. By focusing much on obscenity, the law looks at the morphed image as a threat to public decency, completely ignoring the fact that the victim's identity was stolen and their dignity was violated.

Identity Theft and Cheating Under the Bharatiya Nyaya Sanhita, 2023: Since the law shifted from the old IPC to the Bharatiya Nyaya Sanhita (BNS), prosecutors often use provisions against cheating by impersonation and forgery to target deepfake creators. Under Bharatiya Nyaya Sanhita, editing electronic files can be forgery, and using someone else's face to trick people is called cheating.[14] The structural flaw here is that these laws almost always look like a financial fraud or property loss. In contrast, the deepfakes are usually made to cause emotional trauma, spark political chaos or cause mental harassment. These situations where money does not directly play a role, but the current laws give importance to money. The BNS views these acts through the lens of old-school property crimes; it completely misses the unique constitutional damage of digital identity theft.

The Digital Personal Data Protection Act: As India's newest data privacy shield, the DPDPA 2023 introduces a modern framework for handling digital data, but its applications to deepfakes are highly experimental. Under Sections 4 and 6 of the Act, personal data can only be processed with the free and specific consent.[15] Since deepfakes rely heavily on processing a person's actual biometric data, like their facial structure and voice, creating an unauthorised clone is a clear violation of the consent rule. Additionally, Section 12 gives individuals the right to demand the immediate erasure of their data.[16] This means a victim could legally force an AI

[12] Information Technology Act 2000, s 66E
[13] *Ibid* ss 67–67A
[14] Bharatiya Nyaya Sanhita 2023, s 318, 319 and 336
[15] Digital Personal Data Protection Act 2023, ss 4, 6
[16] *Ibid* s 12

company or platform to delete their deepfake profile. The DPDPA ignores the real-world impacts of AI use. Instead, it prioritises corporate data security over the victims.

Intermediary Liability and IT Rules: These deepfakes spread so fast on media platforms like Instagram, YouTube, and face huge pressure to control them under the IT rules. The government recently shortened the original 36-hour take-down window to just three hours for fake media and two hours for sexually explicit content.[17] While spreads protect victims on paper, it is a nightmare to enforce in real life. Such tight deadlines force platforms to make very hasty decisions about whether the video is real or fake.[18] The platforms lack the tools to instantly spot the difference between a fake and a real video; they face a risky choice: leave the video up and face legal trouble, or play it safe by deleting legitimate content.[19]

CONCLUSION

The quick rise of deepfakes has shown that India's current laws are not ready. Right now, the acts like BNS,[20] the IT Act,[21] and the new IT rules.[22] They are just quick fixes. Instead of relying on this messy mix of rules, the government needs to build a solid legal shield made just for artificial intelligence. This means shifting focus toward stopping harms from happening. Future rules must force platforms and creators to clearly tag or watermark AI content. More importantly, the law must place the victim's peace of mind and personal dignity at the absolute centre of the conversation. True digital safety will only happen when they stop chasing new technology with the old rules and start writing them for the modern world.

[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021; 'Govt notifies AI content rules: AI labels mandatory, 3-hour takedown window on social media' (*BestMediaInfo*, 10 February 2026) <https://bestmediainfo.com/mediainfo/mediainfo-digital/govt-notifies-ai-content-rules-ai-labels-mandatory-3-hour-takedown-window-on-social-media-11094081> accessed 08 May 2026

[18] Aayushman Gaikwad and Smruti Mishra, 'Three Hours To Comply: India's New Rules For AI-Generated Content And Deepfakes' (*Live Law*, 21 February 2026) <https://www.livelaw.in/articles/ai-generated-content-deepfakes-524064> accessed 08 May 2026

[19] Vijay Pal Dalmia, 'India IT Rules Before and After Amendment & AI-Generated Content' (*Vaish Associates*, 24 February 2026) <https://www.vaishlaw.com/india-it-rules-before-and-after-amendment-ai-generated-content/> accessed 08 May 2026

[20] Bharatiya Nyaya Sanhita 2023, ss 318, 319, 336

[21] Information Technology Act 2000, ss 66E, 67, 67A

[22] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021; 'Govt notifies AI content rules: AI labels mandatory, 3-hour takedown window on social media' (n 19)