

CHAPTER 7

Deepfakes and Article 21 of the Indian Constitution: A Case for Legislative Intervention

Mayuri Ramchandra Taware and Onkar A. Wable

in *Law in Transition: Rights, Sovereignty and Regulation in a Changing World*, edited by Siddharth Saxena and Bhagyashree Agarwal (VidhiAagaz 2026), pp. 77–83

DOI <https://doi.org/10.63108/VAB.LIT.1.7>



CITATIONS

BLUEBOOK (21ST ED.)

Mayuri Ramchandra Taware & Onkar A. Wable, *Deepfakes and Article 21 of the Indian Constitution: A Case for Legislative Intervention*, in *LAW IN TRANSITION: RIGHTS, SOVEREIGNTY AND REGULATION IN A CHANGING WORLD* 77 (Siddharth Saxena & Bhagyashree Agarwal eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

Mayuri Ramchandra Taware and Onkar A. Wable, 'Deepfakes and Article 21 of the Indian Constitution: A Case for Legislative Intervention' in Siddharth Saxena and Bhagyashree Agarwal (eds), *Law in Transition: Rights, Sovereignty and Regulation in a Changing World* (VidhiAagaz 2026) 77.

CHICAGO (17TH ED.)

Taware, Mayuri Ramchandra, and Onkar A. Wable. "Deepfakes and Article 21 of the Indian Constitution: A Case for Legislative Intervention." In *Law in Transition: Rights, Sovereignty and Regulation in a Changing World*, edited by Siddharth Saxena and Bhagyashree Agarwal, 77–83. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LIT.1.7>.

APA (7TH ED.)

Taware, M. R., & Wable, O. A. (2026). Deepfakes and article 21 of the Indian constitution: A case for legislative intervention. In S. Saxena & B. Agarwal (Eds.), *Law in transition: Rights, sovereignty and regulation in a changing world* (pp. 77–83). VidhiAagaz. <https://doi.org/10.63108/VAB.LIT.1.7>

SOURCE

<https://doi.org/10.63108/VAB.LIT.1.7>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 7

Deepfakes and Article 21 of the Indian Constitution: A Case for Legislative Intervention

MAYURI RAMCHANDRA TAWARE* AND ONKAR A. WABLE**

Deepfake technology backed by artificial intelligence has transformed the nature of digital harm. Unlike typical misinformation, deepfakes allow for the synthetic alteration of a person's face, voice, gestures, or identity in ways that can jeopardize privacy, dignity, autonomy, reputation, and mental tranquility. These rights are safeguarded under Article 21 of the Indian Constitution, which has been interpreted by judges to encompass the right to privacy, dignity, reputation, and even the right to be left alone. However, India's current legal approach to deepfakes remains fragmented. The Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Digital Personal Data Protection Act, 2023, the Bharatiya Nyaya Sanhita, 2023, and various civil actions, including personality-rights injunctions, offer victims a patchwork of remedies, but they do not constitute a cohesive deepfake law. Thus this paper contends that deepfakes constitute a direct constitutional danger to Article 21, and that India requires a specialized regulatory framework based on permission, provenance disclosure, fast takedown, victim compensation, and platform accountability.

Keywords: Deepfakes, privacy, dignity, reputation, legislative intervention, intermediary liability, Article 21

1 INTRODUCTION

“The danger of deepfakes lies not only in what is fake, but in the doubt they cast on what is real.”

Deepfakes are photos, movies, or sounds that have been manipulated or created with artificial intelligence, AI-powered tools, or audio-video editing software. They may show actual or imaginary persons and are considered a sort of synthetic media, which is typically developed by artificial intelligence systems by integrating diverse media sources into a new media artifact. What makes deepfakes fundamentally significant is not just their deception, but also their ability to steal a person's face, voice, gestures, and social meaning, and then redistribute

* Teaching Faculty at K.C. Law College, Mumbai, Maharashtra, India.

** Advocate at Bombay High Court, Mumbai, Maharashtra, India.

that false identity on an internet scale. In India, the harms include non-consensual sexual images, impersonation fraud, political misinformation, harassment, and reputational damage. The government has noted that deepfakes can adversely harm dignity, reputation, privacy, and platform responsibility whereas current enforcement relies on a mix of the IT Act¹, IT Rules, DPDP Act², and the Bharatiya Nyaya Sanhita.

Article 21 of the Constitution serves as the legal foundation for regulating deepfakes. In *Justice K.S. Puttaswamy v. Union of India*³, the Supreme Court ruled that privacy is inherently linked to life and personal liberty, that privacy safeguards dignity and autonomy, and that informational privacy is a constitutionally protected interest. The Court acknowledged that privacy risks might come from both the state and non-state actors. This conclusion is critical to deepfake regulation because the majority of deepfake damages are created, magnified, or monetized by private actors and platforms rather than the state itself.

This paper contends that India's current legal framework is too fragmented to effectively combat deepfakes. It criminalizes specific aspects of the problem, such as impersonation, obscenity, fraud, and privacy violations, but not synthetic identity harm in general. A dedicated regulation is therefore required, not to prohibit valid satire, art, or political criticism, but to carefully limit malicious synthetic deception in accordance with Articles 19 and 21 of the Indian Constitution.

2 CONSTITUTIONAL HARM CAUSED BY DEEPFAKES UNDER ARTICLE 21

Article 21 has grown from a narrow safeguard against executive deprivation to a comprehensive source of substantive rights linked to a dignified existence. In a nine-judge constitution bench, the Apex Court in the landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) held that the right to privacy is a fundamental right protected under Article 21 of the Constitution and marked the pinnacle of this evolutionary process. The right to privacy is not absolute, but can be limited if such restrictions serve legitimate state interests and are necessary and proportional. This principle is significant for deepfake legislation because it indicates that limits on deepfake creation and dissemination can be constitutionally acceptable provided they protect privacy and dignity while staying reasonable. The Court also declared that privacy protects “the inner recesses of the human personality,” vital life choices, and forms the constitutional core of human dignity. Deepfakes violate all of these values. They take identity without consent, distort personal agency, and turn the individual into a manipulable data item. The hurt is thus more serious than mere defamation: it

¹ The Information Technology Act, 2000.

² The Digital Personal Data Protection Act, 2023.

³ (2017) 10 SCC 1.

is a type of synthetic personality dispossession. The Puttaswamy ruling stressed the importance of privacy in preserving human dignity and autonomy. A four-part test that covers all fundamental rights is outlined in the ruling. It offers a methodology for evaluating the constitutionality of deepfake legislation. By using appropriate and necessary methods, the test makes sure that limitations are not arbitrary but rather support justifiable state interests. In his ruling, Justice Chandrachud outlined a definition of dignity that goes beyond simply being free from torture or cruel treatment to include the right to be treated equally in society and to have one's fundamental human qualities respected. According to Puttaswamy, autonomy is the ability of people to make basic choices about their identities, lives, and bodies without outside intervention. Deepfakes pose a direct threat to these concepts of dignity and autonomy. Deepfakes violate people's dignity by portraying them as objects for sexual use and deception when they show them in fictitious situations, especially sexual ones, without their consent. They also undermine autonomy by using the individual's image and identity to make fraudulent statements and actions that the individual did not authorize and cannot control. In *Subramanian Swamy v. Union of India*⁴, the Supreme Court ruled that reputation is an intrinsic component of Article 21 and cannot be crucified at the altar of someone else's free expression. Deepfakes accomplish exactly that: they convincingly replicate authenticity, causing reputational injury before the deception is proven. The Subramanian Swamy decision showed that the state's duty to protect constitutional rights must be reasonable, proportionate, and not arbitrary. The court did not require the state to remove all threats to Article 21, but only to take reasonable precautions proportionate to the risk.

The Delhi High Court's decision in *Anil Kapoor v. Simply Life India & Ors*⁵ is one of the most direct Indian judicial responses to AI-enabled identity misuse. The Court prohibited defendants from utilizing Anil Kapoor's name, likeness, picture, voice, and personality with Artificial Intelligence, Machine Learning, deep fakes, face morphing, GIFs and other techniques. It acknowledged that technology capabilities today allow illicit users to impersonate celebrities, emphasizing that such misuse jeopardizes privacy, dignity, livelihood, and individuality. The Court said that fame and reputation can harm rights like the right to livelihood, the right to privacy, and the right to live with dignity enumerated under Article 21 of the Indian Constitution. The case also demonstrated how intellectual property rights over personal characteristics have other dimensions including rights protected by the Constitution of India. The Anil Kapoor case is significant because it marks the first time the Indian Supreme Court has directly addressed deepfakes as a constitutional issue. The Court's

⁴ *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221.

⁵ *Anil Kapoor v. Simply Life India*, CS(COMM) 652 of 2023 (Del. HC Sept. 20, 2023).

willingness to hear petitions challenging deepfakes and offer interim remedies indicates that deepfakes create major constitutional problems.

One of the most well-known instances of gendered AI harm in India is the Rashmika Mandanna deepfake event⁶. A video of another lady was altered to include her face, and the fake video became viral on the internet. The Rashmika event is a prime example of privacy, autonomy, and dignity being infringed simultaneously from the standpoint of Article 21. Therefore, the case serves as an example of how deepfake injuries might be articulated constitutionally as infringement of the right to control one's identity and bodily image. The incident also represents a violation of Article 21's right to privacy. The improper collection, analysis, and manipulation of Mandanna's biometric data violated her informational privacy. The dissemination of fake sexualized images of Mandanna violated her right to manage information about herself.

The Sachin Tendulkar case⁷ exemplifies a distinct dimension, fake endorsement and reputational-commercial deceit. A deepfake video made it appear that Tendulkar was advertising a gaming application. According to reports, Mumbai police have filed a case against the gaming website and Facebook page in question. In this case, the hurt was not intimate-image abuse, but rather the manipulation of public trust and identity for financial benefit. The fact that such incidents require piecing together remedies through fraud, defamation, and cybercrime legislation demonstrates the lack of a unified deepfake law.

The deepfake incident involving Asha Bhosle highlighted the growing use of artificial intelligence to imitate a person's voice and likeness without their consent. Manipulated content fraudulently depicted her in situations in which she had no involvement, creating major concerns about identity theft and digital impersonation. The court awarded relief by prohibiting the transmission of such content, recognizing that unauthorized use of voice and persona breaches personality rights, which are inextricably tied to the right to privacy and dignity guaranteed by Article 21 of the Constitution. The case highlights the inadequacies of existing legal frameworks and reinforces the need for separate legislation to regulate deepfakes in India⁸.

⁶ *Rashmika Mandanna Deepfake Video Sparks Debate on AI Misuse*, HINDU (Nov. 6, 2023), <https://www.thehindu.com>.

⁷ *Deepfake Video of Sachin Tendulkar Promoting Gaming App Triggers Police Action*, INDIAN EXPRESS (Jan. 17, 2024), <https://indianexpress.com>.

⁸ *Music Legend Asha Bhosle Sues AI Firm and E-Commerce Sites over Voice and Image Misuse*, MONDAQ (Oct. 8, 2025), <https://www.mondaq.com/india/copyright/1688044/music-legend-asha-bhosle-sues-ai-firm-and-e-commerce-sites-over-voice-and-image-misuse>.

3 THE EXISTING LEGAL FRAMEWORK

Although Article 21 provides the constitutional basis for contesting deepfake harms in India, legislative and regulatory tools play a major role in practical enforcement. These include the Bharatiya Nyaya Sanhita (2023), the Digital Personal Data Protection Act (2023), the Information Technology Act (2000), and the IT Rules. However, rather than regulating deepfakes as a separate category of synthetic identity abuse, these laws primarily deal with the consequences of deepfakes, such as privacy violations, personation, obscenity, fraud, defamation, or false records. This results in a reactive legal system where victims frequently have to fit a single technology injury into multiple outdated legal categories.

The IT Act of 2000 remains the primary statutory weapon for addressing the harms produced by deepfakes. According to government explanations, the Act already encompasses acts such as identity theft, personation fraud, privacy violations, and the publication or transfer of obscene or sexually explicit information. In practice, rules often linked with these harms such as those dealing with privacy, impersonation, and obscene material are invoked when deepfakes are exploited for fraud, false endorsements, sexual exploitation, or reputational harm. Deepfakes made for fraud or impersonation may be covered by Section 66D of the IT Act, which deals with cheating by personation through computers or the internet. Deepfakes that show non-consensual intimate imagery may be subject to Section 67 of the IT Act, which deals with indecent dissemination. However, the problem is that the statute does not explicitly define or control deepfakes or synthetic media; instead, it captures them indirectly through pre-existing crime categories.

The intermediary framework established by the IT Rules has moved more directly toward deepfake governance. Previously, government recommendations regarded deepfakes as a type of illegal misinformation, requiring platforms to exercise caution in blocking and removing such content. More recently, official MeitY materials on revisions to synthetically generated information imposed stricter requirements, such as user declarations, visible labels, metadata or provenance identifiers, and quicker grievance resolution.

The Bharatiya Nyaya Sanhita, 2023, contains laws related to voyeurism, sexual harassment, and insult to modesty that may be used to combat specific types of malicious deepfake abuse, including non-consensual intimate imagery directed at women. Section 500 of the IPC and Section 356 of the BNS both deal with defamation. The BNS's Sections 67 and 67A deal with pornographic publications and images of children, and they may apply to deepfakes. Nevertheless, neither the BNS nor the IPC specifically addresses deepfakes as a separate harm category. Because ordinary defamation and obscenity laws do not address the unique mechanisms and harms caused by deepfake technology, their application to deepfakes is still insufficient.

4 THE CASE FOR LEGISLATIVE INTERVENTION

The first step in creating a specific deepfake law in India should be to clearly identify deepfake injury as a matter of privacy, autonomy, dignity, reputation, and informational integrity under Article 21. This would recast victims as rights-holders whose constitutional interests are directly harmed by synthetic media, rather than just as platform complainants. The law should include explicit definitions. It must differentiate between synthetically generated information, deepfakes, voice clones, face swaps, manipulative political material, consensual synthetic media, satire, parody, and creative transformation. Overbreadth would endanger free expression, while underbreadth would leave victims vulnerable. Following democratic debate, these boundaries should be established in a statute.

The law should establish a graded harm model. Non-consensual intimate deepfakes, child sexual abuse deepfakes, fraud deepfakes, election manipulation deepfakes, and forged official papers should be considered as aggravated offenses with harsher punishments and faster remedies. In contrast, lower-risk categories may be governed through labeling and disclosure rather than restriction. This method would more closely align legal responses with constitutional proportionality. India needs quick and victim-centered solutions. A new law should include emergency takedown orders, time-bound grievance resolution, evidence preservation, protection against re-uploading, search de-indexing where appropriate, and compensation for proven injury. Victim anonymity should be provided in sexual deepfake situations. These are aspects that cannot be left to randomly distributed platform policies and wide criminal provisions alone.

5 CONCLUSION

Deepfakes are more than just a technological inconvenience or a new type of online mischief: they are an outright attack on constitutional personhood. When confronted with synthetic manipulation, they undercut the individual's authority over identity, erode trust in true expression, and highlight the limitations of existing legal categories. Legislative involvement is therefore no longer an option. It is a constitutional requirement for Indian law to genuinely defend privacy, dignity, autonomy, reputation, and personality rights in the age of artificial intelligence. However, the current legal response is fragmented, relying on a hodgepodge of privacy, obscenity, impersonation, data protection, and intermediary liability provisions that only address a portion of the harm. This doctrinal and regulatory gap warrants specific legislative action. Any future regulation must precisely identify deepfakes, provide timely victim-centered remedies, enforce appropriate platform requirements, and

demand transparency measures such as provenance or disclosure, while being consistent with free expression safeguards.

* * *