



# The Indian Journal for Research in Law and Management

Open Access Law Journal–Copyright©2026

Editor-in-Chief–Dr. Muktai Deb Chavan; Publisher– Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

## THE RIGHT TO BE REAL: LEGAL CHALLENGES POSED BY DEEPPAKES AND AI-GENERATED MEDIA

*When Seeing Is No Longer Believing, The Law Must Protect The Right To  
Reality*

~ Tanu Agrawal

### ABSTRACT

*The proliferation of deepfakes and AI-generated synthetic media poses unprecedented challenges to individual rights, democratic integrity, and the rule of law in India. This paper examines the legal landscape governing deepfakes, identifying critical gaps in existing frameworks including the Bhartiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and the recently notified IT Amendment Rules, 2026. Through doctrinal legal research, the study analyses how current provisions inadequately address the unique harms of synthetically generated information (SGI), particularly concerning personality rights, privacy under Article 21, and electoral manipulation. The research reveals that while the 2026 Rules introduce mandatory labeling and accelerated takedown mechanisms; they remain reactive and platform-centric, lacking a comprehensive statutory offence for malicious deepfake creation. The paper proposes a dedicated legislative framework incorporating pre-emptive verification, civil liability for creators, and enhanced forensic infrastructure, drawing comparative insights from the EU AI Act and international best practices.*

**Keywords:** Deepfakes, Synthetically Generated Information, Article 21, IT Rules 2026, Personality Rights, Electoral Integrity.

## I. INTRODUCTION

### A. Background and Context

The advent of generative artificial intelligence has democratised the creation of hyper-realistic synthetic media, commonly termed "deepfakes".<sup>1</sup> These audio, visual, or audio-visual representations, artificially generated or algorithmically altered to appear authentic, have evolved from novelty entertainment to instruments of significant societal harm.<sup>2</sup> In India, the 2024 Lok Sabha elections witnessed the deployment of deepfakes to manipulate voter perceptions, fabricate political statements, and discredit opponents, raising urgent concerns about electoral integrity and democratic discourse.<sup>3</sup>

The technological sophistication of deepfakes now enables near-perfect impersonation of public figures, judicial officers, and private citizens alike.<sup>4</sup> High-profile incidents, including the Rashmika Mandanna deepfake case (2023) and fabricated audio clips of political leaders during state elections, demonstrate the ease with which malicious actors can exploit synthetic media for extortion, defamation, and disinformation.<sup>5</sup> The Supreme Court's landmark recognition of privacy as a fundamental right under Article 21 in *K.S. Puttaswamy v. Union of India* provides a constitutional anchor for addressing these violations, yet statutory frameworks remain fragmented and reactive.<sup>6</sup>

<sup>1</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), 10.02.2026 (effective 20.02.2026) <https://egazette.gov.in/WriteReadData/2026/269993.pdf> accessed on 18 August 2026; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (updated Feb. 10, 2026), <https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf>.

<sup>2</sup> *Ibid.*; Deepfakes, Due Diligence And The Good Samaritan Paradox, LIVE LAW (Apr. 14, 2026), <https://www.livelaw.in/law-firms/law-firm-articles/-/deepfakes-due-diligence-indias-2026-it-amendment-rules-resolve-global-platfo>.

<sup>3</sup> Deepfake Cases in the 2024 Lok Sabha Election: Impact and Implications, 5(22553) IJFMR (2024), <https://www.ijfmr.com/papers/2024/5/22553.pdf>; Election Comm'n of India, *Advisory on Ethical Use of Social Media and Deepfakes in Elections*, No. 491/SM SOP/2024/Communication (May 6, 2024), <https://elections24.eci.gov.in/docs/2eJLvv9x2w.pdf> accessed on 18 August 2026.

<sup>4</sup> Deepfake Technology and Its criminal misuse, 12(2) LAW JOURNALS (2026), <https://www.lawjournals.org/assets/archives/2026/vol12issue2/12154.pdf>; Ian J. Goodfellow et al., Generative Adversarial Nets, in *Advances in Neural Information Processing Systems* 2672, 2672–80 (2014), <https://papers.nips.cc/paper/5423-generative-adversarial-nets> accessed on 18 August 2026.

<sup>5</sup> Swati Bansal, *Creator of Deepfake Video of Actor Rashmika Mandanna Arrested, Says Delhi Police*, The Hindu (Jan. 20, 2024), <https://www.thehindu.com/sci-tech/technology/creator-of-deepfake-video-of-actor-rashmika-mandanna-arrested-says-delhi-police/article67759285.ece> accessed on 18 August 2026.

<sup>6</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1, <https://indiankanoon.org/doc/91938676/>.

## B. Statement of the Problem

India's legal response to deepfakes has been characterised by legislative inertia and regulatory patchwork.<sup>7</sup> While the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026 and effective from 20 February 2026, introduce the first comprehensive statutory framework for "synthetically generated information" (SGI), critical gaps persist.<sup>8</sup> The Rules impose labeling obligations, metadata embedding requirements, and accelerated takedown timelines (3 hours for certain categories), yet they primarily target intermediaries rather than creators of malicious content.<sup>9</sup>

The absence of a standalone criminal offence for deepfake creation, coupled with inadequate penalties under existing provisions of the Bharatiya Nyaya Sanhita, 2023 (BNS) and the IT Act, 2000, renders enforcement ineffective.<sup>10</sup> Sections 319 (cheating by personation), 356 (defamation), and 336 (organised cyber crime) of the BNS, alongside Sections 66C (identity theft), 66D (impersonation), and 67 (obscene material) of the IT Act, provide indirect remedies but fail to address the unique epistemic and dignitary harms of synthetic media.<sup>11</sup>

## C. Research Gap

Existing scholarship on deepfakes in India predominantly focuses on doctrinal analysis of pre-2026 legal frameworks, identifying the "legal vacuum" without proposing concrete legislative solutions.<sup>12</sup> Recent articles in the Indian Journal for Research in Law and Management (IJRLM) examine the adequacy of cyber law frameworks and the BNS's

<sup>7</sup> *Deepfakes in India: Legal provisions, challenges and way forward*, 11(12) LAW JOURNALS (2025), <https://www.lawjournals.org/assets/archives/2025/vol11issue12/11315.pdf>; Jyothsna Gurumurthy, *In the Pursuance of a Robust Legal Framework to Address Deepfake Harms: An Analysis of the Indian Legal Discourse*, 20 Indian J. L. & Tech., no. 1, art. 1 (2024), <https://repository.nls.ac.in/ijlt/vol20/iss1/1/>, accessed on 18 August 2026.

<sup>8</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (India), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.

<sup>9</sup> Ministry of Electronics & Information Technology, *Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, <https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf>.

<sup>10</sup> *Bharatiya Nyaya Sanhita*, 2023, No. 45, Acts of Parliament, 2023 (India); Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), <https://www.indiacode.nic.in/handle/123456789/1362>.

<sup>11</sup> *Bharatiya Nyaya Sanhita*, 2023, §§ 111, 319, 336, 351, 353, 354, No. 45, Acts of Parliament, 2023 (India); Information Technology Act, 2000, §§ 66C, 66D, 67, No. 21, Acts of Parliament, 2000 (India).

<sup>12</sup> Jyothsna Gurumurthy, *supra* note 7.

applicability to deepfakes, yet they lack comprehensive engagement with the IT Amendment Rules, 2026, and their practical implications.<sup>13</sup>

A critical gap exists in empirical and comparative analysis: no study has systematically evaluated the 2026 Rules' effectiveness against international models such as the EU AI Act's deepfake disclosure obligations or China's mandatory real-name verification for synthetic content creators.<sup>14</sup> Furthermore, the intersection of deepfakes with personality rights, electoral law, and the emerging Digital India Act remains underexplored in Indian legal literature.<sup>15</sup>

#### D. Need for the Study

The urgency of this research is underscored by three factors. First, the exponential growth of AI-generated content: India's millions of internet users are increasingly exposed to synthetic media, though Reliable official Indian statistics isolating deepfake-related offences, prosecutions, and convictions are presently limited. Accordingly, this study does not quantify the national incidence of deepfake crime.<sup>16</sup> Second, the 2026 Rules represent a pivotal regulatory shift, yet their practical efficacy remains untested, necessitating critical scholarly evaluation.<sup>17</sup> Third, the absence of a dedicated deepfake statute leaves victims without adequate civil remedies, particularly in cases of non-consensual deepfake pornography, financial fraud, and political disinformation.<sup>18</sup>

This study addresses these gaps by providing a comprehensive legal analysis, identifying legislative inadequacies, and proposing a rights-based regulatory framework aligned with constitutional values and international best practices.

---

<sup>13</sup> *Adequacy of Indian Cyber Laws in Tackling Deepfake Crimes: A Critical Legal Analysis*, Vistas Institutional Repository (2026), <https://ir.vistas.ac.in/id/eprint/15090/>.

<sup>14</sup> Regulation (EU) 2024/1689, arts. 3(60), 50, 99, 2024 O.J. (L 1689), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>; Cyberspace Administration of China et al., *Provisions on the Administration of Deep Synthesis Internet Information Services* (promulgated Nov. 25, 2022, effective Jan. 10, 2023), [http://www.cac.gov.cn/2022-12/11/c\\_1672221949354811.htm](http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm).

<sup>15</sup> Ministry of Electronics & Information Technology, *Presentation on Digital India Act*, Mar. 9, 2023, [https://www.meity.gov.in/writereaddata/files/DIA\\_Presentation%2009.03.2023%20Final.pdf](https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf).

<sup>16</sup> Data Security Council of India, *Annual Cybercrime and Deepfake Threat Landscape Report 2025*, at 18–22 (2025).

<sup>17</sup> International IDEA, *The Election Year 2024 and Tech Policy Around the World*, <https://www.idea.int/publications/catalogue/html/election-year-2024-and-tech-policy-around-world-what-lessons-european>.

<sup>18</sup> Election Comm'n of India, *Advisory on Ethical Use of Social Media and Deepfakes in Elections*, No. 491/SM\_SOP/2024/Communication (May 6, 2024), <https://elections24.eci.gov.in/docs/2eJLyv9x2w.pdf>.

## **E. Research Objectives**

This paper pursues five interconnected objectives.

- i. *First*, it critically analyses the existing legal framework governing deepfakes and AI-generated synthetic media in India, including the BNS, IT Act, IT Rules 2026, and DPDP Act, 2023.
- ii. *Second*, it identifies legislative lacunae, enforcement challenges, and evidentiary hurdles in addressing deepfake-related harms.
- iii. *Third*, it evaluates the constitutional implications of deepfakes concerning Articles 19 (freedom of speech) and 21 (right to privacy and dignity).
- iv. *Fourth*, it conducts a comparative analysis of international regulatory approaches, including the EU AI Act, US state laws, and China's deepfake regulations.
- v. *Fifth*, it proposes a dedicated legislative framework incorporating pre-emptive verification, creator liability, and enhanced forensic infrastructure.

## **F. Research Questions**

The study addresses five core questions.

- i. How adequate are India's current statutory provisions (BNS, IT Act, IT Rules 2026) in addressing the unique harms of deepfakes and synthetic media?
- ii. What constitutional rights are implicated by deepfake proliferation, and how have Indian courts interpreted personality rights and privacy in this context?
- iii. What enforcement and evidentiary challenges impede effective prosecution of deepfake-related offences?
- iv. How do international regulatory models compare to India's approach, and what lessons can be drawn for legislative reform?
- v. What elements should a comprehensive deepfake-specific legislation include to balance innovation, free expression, and individual rights?

## G. Hypothesis

The hypothesis primarily posits that India's existing legal framework, including the IT Amendment Rules, 2026, is structurally inadequate to address the unique harms of deepfakes, necessitating dedicated legislation that imposes direct liability on creators, mandates pre-publication verification for high-risk content, and establishes specialised forensic infrastructure.

## II. LITERATURE REVIEW

### A. Conceptual Framework: Defining Deepfakes and SGI

The term "*deepfake*" originates from "*deep learning*" and "*fake*", referring to synthetic media generated using generative adversarial networks (GANs) and other AI techniques.<sup>19</sup> The IT Amendment Rules, 2026, define "*synthetically generated information*" (SGI) as "audio, visual or audio-visual information which is artificially or algorithmically created, generated, modified or altered using a computer resource, in a manner that such information appears to be real, authentic or true and depicts or portrays any individual or event in a manner that is, or is likely to be perceived as indistinguishable from a natural person or real-world event".<sup>20</sup>

This definition excludes automatically retouched smartphone photos and film special effects, narrowing the scope to content that could reasonably deceive a person into believing it depicts genuine persons or events. Scholars distinguish between "benign" SGI such as entertainment, satire with disclosure and "malicious" SGI like non-consensual pornography, electoral disinformation, financial fraud).<sup>21</sup>

### B. Existing Scholarship on AI and Law

Indian legal scholarship on deepfakes has evolved through three phases. Phase I (2020–23) focused on identifying the "legal vacuum", highlighting the absence of specific provisions in

<sup>19</sup> Ian J. Goodfellow et al., *Generative Adversarial Nets*, in *Advances in Neural Information Processing Systems* 2672, 2672–80 (2014), <https://papers.nips.cc/paper/5423-generative-adversarial-nets>.

<sup>20</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Rule 2(1)(wa), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.

<sup>21</sup> Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Calif. L. Rev. 1753 (2019), <https://www.jstor.org/stable/26891938>.

the IPC and IT Act.<sup>22</sup> Phase II (2024–25) analysed constitutional dimensions, particularly Article 21's protection of informational privacy and personality rights.<sup>23</sup> Phase III (2026–present) examines the IT Rules, 2026, though comprehensive evaluations remain nascent.<sup>24</sup>

### C. Gaps in Literature

Three critical gaps emerge. First, *post-2026 analysis*: the available literature reviewed for this paper contains limited sustained analysis of the 2026 amendments.<sup>25</sup> Second, *comparative deficit*: limited engagement with international models (EU AI Act's labeling mandates<sup>26</sup>, China's real-name verification for AI content creators).<sup>27</sup> Third, *remedial frameworks*: insufficient attention to civil remedies, particularly for non-consensual deepfake pornography and financial fraud victims.<sup>28</sup> This study addresses these gaps by integrating the 2026 Rules into a comprehensive analysis and proposing a dedicated legislative framework.

## III. METHODOLOGY

### A. Research Design

This study employs a doctrinal legal research methodology, combining qualitative analysis of statutory provisions, judicial precedents, policy documents, and academic literature.<sup>29</sup> The research is analytical and evaluative, assessing the adequacy of existing laws against the unique challenges posed by deepfakes. Doctrinal analysis enables systematic examination of legal texts, judicial reasoning, and regulatory frameworks, providing a foundation for identifying gaps and proposing reforms.

<sup>22</sup> Jyothsna Gurumurthy, *In the Pursuance of a Robust Legal Framework to Address Deepfake Harms: An Analysis of the Indian Legal Discourse*, 20 Indian J. L. & Tech., no. 1, art. 1 (2024), <https://repository.nls.ac.in/ijlt/vol20/iss1/1/>.

<sup>23</sup> *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914, <https://recordoflaw.in/anil-kapoor-v-simply-life-india-ors-2023-personality-rights-in-the-age-of-artificial-intelligence/>.

<sup>24</sup> *Adequacy of Indian Cyber Laws in Tackling Deepfake Crimes: A Critical Legal Analysis*, Vistas Institutional Repository (2026), <https://ir.vistas.ac.in/id/eprint/15090/>.

<sup>25</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E) (India), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.

<sup>26</sup> Regulation (EU) 2024/1689, arts. 3(60), 50, 2024 O.J. (L 1689), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

<sup>27</sup> Cyberspace Administration of China et al., *Provisions on the Administration of Deep Synthesis Internet Information Services* (promulgated Nov. 25, 2022, effective Jan. 10, 2023), [http://www.cac.gov.cn/2022-12/11/c\\_1672221949354811.htm](http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm).

<sup>28</sup> *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914, <https://recordoflaw.in/anil-kapoor-v-simply-life-india-ors-2023-personality-rights-in-the-age-of-artificial-intelligence/>. Jyothsna Gurumurthy, *In the Pursuance of a Robust Legal Framework to Address Deepfake Harms: An Analysis of the Indian Legal Discourse*, 20 Indian J. L. & Tech., no. 1, art. 1 (2024), <https://repository.nls.ac.in/ijlt/vol20/iss1/1/>.

<sup>29</sup> Terry Hutchinson, *Researching and Writing in Law* (4th ed. 2018).

## B. Sources of Data

**Primary Sources:** The study draws upon statutes including the Bharatiya Nyaya Sanhita, 2023;<sup>30</sup> Information Technology Act, 2000;<sup>31</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026;<sup>32</sup> and Digital Personal Data Protection Act, 2023.<sup>33</sup> Judicial precedents include *K.S. Puttaswamy v. Union of India* (2017); *R. Rajagopal v. State of T.N.* (1995); and Delhi High Court rulings on personality rights and deepfakes (2023–2026).<sup>34</sup> Government notifications, particularly MeitY's IT Amendment Rules, 2026 (G.S.R. 120(E), 10.02.2026), provide the regulatory baseline.<sup>35</sup>

**Secondary Sources:** Peer-reviewed journal articles from Indian Journal for Research in Law and Management (IJRLM), Indian Journal of Legal Research (IJLR), Indian Journal of Advanced Legal Research (IJALR), and other law reviews inform the analysis. Policy reports from the Data Security Council of India and CIVICUS DDI Research (2025)<sup>36</sup> offer empirical context. News analyses and case studies from BOOM Live Deepfake Tracker, Rest of World, and law journal articles provide real-world examples.<sup>37</sup>

## C. Limitations

Three limitations constrain this study. First, empirical data scarcity: limited official statistics on deepfake prosecutions and convictions in India restrict quantitative analysis.<sup>38</sup> Second, the evolving regulatory landscape: the IT Rules, 2026, being newly notified, lack judicial

<sup>30</sup> *Bharatiya Nyaya Sanhita*, 2023, No. 45, Acts of Parliament, 2023 (India).

<sup>31</sup> Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), <https://www.indiacode.nic.in/handle/123456789/1362>.

<sup>32</sup> Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), <https://www.indiacode.nic.in/handle/123456789/1362>.

<sup>33</sup> Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

<sup>34</sup> *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1; *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632; *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914.

<sup>35</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E) (India), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.

<sup>36</sup> *Civics DDI Research, Future-Proofing Elections Against Deepfake Disinformation* (2025), <https://www.civics.org/documents/ddi/final-deepfakes-elections-report-civics-ddi-research-2025.pdf>.

<sup>37</sup> General Elections And Bye-Elections 2026: ECI Action On Unlawful Social Media Content, Election Commission (19 April 2026) <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2253528&reg=3&lang=1>.

<sup>38</sup> National Crime Records Bureau, *Crime in India 2024*, Ministry of Home Affairs, Government of India (2025).

interpretation and enforcement data.<sup>39</sup> Third, technological complexity: rapid advancements in AI may outpace the analysis, requiring continuous updates to the framework.

#### IV. LEGAL FRAMEWORK IN INDIA

##### A. Constitutional Provisions

- i. *Article 21 (Right to Life and Personal Liberty)*: In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a constitutionally protected fundamental right under Article 21. The judgment's discussion includes decisional autonomy, dignity, and informational privacy.<sup>40</sup> Deepfakes may implicate privacy, dignity, autonomy, reputation, and control over a person's identity or likeness; however, whether a particular deepfake violates Article 21 depends on the facts and the legal remedy invoked.<sup>41</sup>
- ii. *Article 19(1)(a) (Freedom of Speech and Expression)*: Synthetic media may constitute protected expression in some circumstances, including parody, satire, art, or political commentary. In *Shreya Singhal v. Union of India*, the Supreme Court distinguished discussion and advocacy from incitement and held that restrictions on speech must fall within the grounds specified in Article 19(2).<sup>42</sup> A malicious deepfake is not automatically outside Article 19(1)(a); its regulation must still satisfy constitutional requirements of legality, reasonableness, and proportionality.<sup>43</sup>
- iii. *Article 19(2) (Reasonable Restrictions)*: Article 19(2) permits reasonable restrictions on speech in the interests of the sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, decency or morality, contempt of court, defamation, or incitement to an offence.<sup>44</sup> Any restriction directed at deepfakes must pursue a legitimate purpose, bear a rational connection to that

<sup>39</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E) (India), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.

<sup>40</sup> *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, <https://indiankanoon.org/doc/91938676/>.

<sup>41</sup> *Id.*; see also Constitution of India art. 21, <https://legislative.gov.in/constitution-of-india/>.

<sup>42</sup> *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, <https://recordoflaw.in/shreya-singhal-v-union-of-india-2015/>.

<sup>43</sup> *Id.*; see also INDIA CONST. arts. 19(1)(a), 19(2), <https://legislative.gov.in/constitution-of-india/>.

<sup>44</sup> INDIA CONST. art. 19, cl. 2, <https://legislative.gov.in/constitution-of-india/>.

purpose, be necessary and suitably tailored, and maintain a fair balance between the right and the public interest.<sup>45</sup>

## **B. Bharatiya Nyaya Sanhita, 2023**

The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal Code with effect from 1 July 2024. Its provisions may apply to particular deepfake-related conduct, but the Sanhita does not create a general, standalone offence of “deepfake creation.”<sup>46</sup> Section 111 concerns organised crime and may apply only where the statutory ingredients of organised crime are established; it does not automatically cover every group involved in producing or circulating deepfakes.<sup>47</sup> Section 319 concerns cheating by personation and may be relevant where a person uses a deepfake to deceive another by personation. Its application depends on proof of the statutory elements, including deception and dishonest or fraudulent inducement.<sup>48</sup> Section 336 concerns forgery, including the making of a false document or false electronic record with the specified intent. It may be relevant to a synthetic or manipulated electronic record only where the statutory requirements of forgery are satisfied.<sup>49</sup>

Section 351 concerns criminal intimidation and may apply where threatening deepfake content satisfies the elements of that offence.<sup>50</sup> Section 353 concerns statements conducing to public mischief and may apply to false information, rumours, or reports circulated electronically in the circumstances specified by the section. It should not be described generally as the offence of defamation.<sup>51</sup> Section 354 concerns imputations, assertions, or prejudicial allegations affecting national integration and must be applied according to its precise statutory language; it should not be treated as a general communal-harmony provision for all deepfakes.<sup>52</sup>

---

<sup>45</sup> *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353, <https://indiankanoon.org/doc/151348870/>.

<sup>46</sup> *Bharatiya Nyaya Sanhita*, 2023, No. 45, Acts of Parliament, 2023 (India), <https://www.indiacode.nic.in/handle/123456789/1362>.

<sup>47</sup> *Bharatiya Nyaya Sanhita*, 2023, § 111, No. 45, Acts of Parliament, 2023 (India), <https://www.indiacode.nic.in/handle/123456789/1362>.

<sup>48</sup> *Id.* § 319.

<sup>49</sup> *Id.* § 336.

<sup>50</sup> *Bharatiya Nyaya Sanhita*, 2023, § 351, No. 45, Acts of Parliament, 2023 (India), <https://www.indiacode.nic.in/handle/123456789/1362>.

<sup>51</sup> *Id.* § 353.

<sup>52</sup> *Id.* § 354.

These provisions may provide fact-specific routes to prosecution, but they do not comprehensively regulate synthetic media. The absence of a deepfake-specific offence may create difficulties concerning mens rea, attribution, authenticity, causation, and the classification of manipulated media.<sup>53</sup>

### C. Information Technology Act, 2000

The Information Technology Act, 2000 contains provisions that may apply to particular forms of deepfake-related conduct. Section 66C concerns identity theft involving the fraudulent or dishonest use of another person's electronic signature, password, or other unique identification feature, and carries imprisonment of up to three years and a fine of up to ₹1 lakh.<sup>54</sup> Section 66D concerns cheating by personation using a communication device or computer resource and carries imprisonment of up to three years and a fine of up to ₹1 lakh.<sup>55</sup>

Sections 67, 67A, and 67B address the publication or transmission of obscene material, sexually explicit material, and material depicting children in sexually explicit acts or conduct, respectively. Whether a deepfake falls within any of these provisions depends on its content, the manner of publication or transmission, and the statutory elements of the relevant offence.<sup>56</sup>

Section 79 provides conditional safe-harbour protection for intermediaries, subject to the statutory requirements and applicable due-diligence obligations. It does not provide an absolute defence to platforms, nor does it impose general criminal liability merely because unlawful content is uploaded by a user.<sup>57</sup> The Act was enacted before contemporary generative-AI systems emerged, so its application to synthetic media requires careful, provision-specific analysis rather than broad assumptions.<sup>58</sup>

---

<sup>53</sup> *Id.* §§ 319, 336, 351, 353; Information Technology Act, 2000, §§ 66C, 66D, 67, 67A, 67B, 79, No. 21, Acts of Parliament, 2000 (India).

<sup>54</sup> Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India).

<sup>55</sup> *Id.* § 66D.

<sup>56</sup> *Id.* §§ 67, 67A, 67B. See also Press Information Bureau, *India Well-Equipped to Tackle Evolving Online Harms and Cyber Crimes*, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268&reg=3&lang=1>

<sup>57</sup> Information Technology Act, 2000, § 79, <https://www.indiacode.nic.in/handle/123456789/1362>.

<sup>58</sup> *Id.* §§ 2(1)(t), 79.

## D. IT Amendment Rules, 2026

Notified on 10 February 2026, these Rules represent India's first comprehensive SGI regulatory framework.<sup>59</sup> Rule 2(1)(wa) defines SGI as audio, visual, and audio-visual content created or altered through AI or algorithmic processes to appear convincingly real.<sup>60</sup> Rule 3(3) imposes due diligence obligations on intermediaries. They must implement "reasonable and appropriate technical measures" to prevent unlawful SGI.<sup>61</sup> Permissible SGI must carry prominent labels and embedded metadata with unique identifiers tracing origin and alterations. Tools enabling label or metadata removal are prohibited.

Rule 4(1A) imposes additional obligations on Significant Social Media Intermediaries (SSMIs). They must obtain user declarations on whether content is SGI and deploy technical measures to verify declarations before publication.<sup>62</sup> Confirmed SGI must carry visible disclosure tags. Accelerated takedown timelines require certain high-risk SGI categories, for instance, deepfakes impersonating public figures, electoral disinformation) to be removed within 3 hours.<sup>63</sup>

Rule 2(1B) clarifies safe harbour implications: intermediaries removing SGI in compliance with the Rules will not lose protection under Section 79(2)(a) or (b) of the IT Act, regardless of whether removal was human or automated.<sup>64</sup> The Rules target intermediaries, not creators. They lack criminal penalties for malicious deepfake creation and rely on platforms' technical capacity for verification, which varies widely.

The Rules regulate intermediary conduct and due diligence; they do not, by themselves, create a general criminal offence applicable to every person who creates a deepfake. Any criminal liability of a creator must therefore be established under another applicable statute, such as the BNS or the IT Act, depending on the facts.<sup>65</sup>

---

<sup>59</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E) (India), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.

<sup>60</sup> *Id.* r. 2(1)(wa).

<sup>61</sup> *Id.* r. 3(3).

<sup>62</sup> IT Amendment Rules, 2026, r. 4(1A).

<sup>63</sup> *Id.* r. 3(1)(b).

<sup>64</sup> *Id.* r. 2(1B).

<sup>65</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>; *Bharatiya Nyaya Sanhita*, 2023, No. 45, Acts of Parliament, 2023 (India); see also Ministry of Electronics & Information Technology, *Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code)*

## E. Digital Personal Data Protection Act, 2023

The DPDP Act, 2023, though primarily focused on personal data, offers ancillary protections, thus, it may become relevant where the creation, use, or dissemination of synthetic media involves the processing of digital personal data.<sup>66</sup> It treats biometric data (face, voice, etc.) as personal data but does not create a separate “sensitive biometric” regime. Its main relevance is to require a lawful basis (usually consent) for using personal data in deepfake generation and to impose data-fiduciary duties regarding notice, purpose limitation, security safeguards, and breach response.<sup>67</sup>

Following are few key sections for deepfakes and biometric data:

- *Section 2(t)*: defines “personal data” as any data about an individual who is identifiable by or in relation to such data (covers face, voice, and other biometric-linked data when identifiable).
- *Section 4*: sets the grounds for processing personal data (consent or specified legitimate uses); this is the main provision that makes unauthorised use of a person’s image or voice in a deepfake potentially unlawful.
- *Section 8*: imposes data-fiduciary obligations, including notice, purpose limitation, data quality, security safeguards, and breach response; relevant to AI developers, platforms, and studios that determine the purpose and means of processing personal data for deepfakes.

## F. Judicial Precedents on Personality Rights and Privacy

Indian courts have increasingly recognised personality rights as an aspect of privacy, dignity, and reputation under Article 21, even though no standalone statutory “right of publicity” exists.<sup>68</sup> The Supreme Court’s decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* recognises privacy as a constitutionally protected fundamental right, encompassing

---

*Amendment Rules, 2026,*

<https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf>.

<sup>66</sup> Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>.

<sup>67</sup> *Ibid*, §§ 2(t), 4, 8, <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>.

<sup>68</sup> See *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914; *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

informational privacy, dignity, and decisional autonomy.<sup>69</sup> While *Puttaswamy* is not a deepfake or personality-rights judgment *per se*, it provides the constitutional foundation for protecting an individual's control over their identity, image, and voice against unauthorised digital manipulation.<sup>70</sup>

In *R. Rajagopal v. State of T.N.*, the Supreme Court recognised the right to privacy as implicit in Article 21 and clarified the balance between privacy, reputation, and freedom of expression, particularly in the context of publication of personal information.<sup>71</sup> The judgment is often relied upon to support the proposition that unauthorised publication or exploitation of aspects of a person's identity may violate privacy and reputation, thereby recognising the right to control publication of one's image, laying groundwork for personality rights.<sup>72</sup>

More directly relevant to deepfakes and AI-generated synthetic media are recent Delhi High Court decisions protecting personality rights against unauthorised digital use. In *Anil Kapoor v. Simply Life India*, the Delhi High Court granted an omnibus injunction restraining multiple entities and "John Doe" defendants from using the actor's name, image, voice, likeness, and other attributes of his persona, including through AI, deepfakes, face-morphing, and voice-cloning technologies.<sup>73</sup> The Court recognised that personality rights extend beyond static image or name to include distinctive gestures, manner of speaking, and other identifiable attributes, and that unauthorised AI-enabled replication may cause reputational, emotional, and commercial harm.<sup>74</sup> Similar interim orders have since been granted in favour of other public figures, including Khushi Kapoor, Hrithik Roshan, and Ankur Warikoo, reflecting a judicial trend towards robust, technology-neutral protection of personality rights against AI-driven impersonation.<sup>75</sup>

<sup>69</sup> □ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, <https://indiankanoon.org/doc/91938676/>.

<sup>70</sup> *Id.*; see also Constitution of India art. 21, <https://legislative.gov.in/constitution-of-india/>.

<sup>71</sup> *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632, <https://indiankanoon.org/docfragment/501107/?formInput=%20%20right%20to%20privacy>.

<sup>72</sup> *Id.*; see also *Khurana & Khurana*, Personality Rights & AI Cloning: Legal Gaps in India (Sept. 9, 2025), <https://www.khuranaandkhurana.com/personality-rights-in-peril-addressing-ai-generated-cloning-through-indian-legal-frameworks>.

<sup>73</sup> *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914, <https://recordoflaw.in/anil-kapoor-v-simply-life-india-ors-2023-personality-rights-in-the-age-of-artificial-intelligence/>.

<sup>74</sup> *Id.*; see also LiveLaw, Personality Rights: Celebrity Rights Or Case For Identity Theft? (Mar. 12, 2026), <https://www.livelaw.in/law-firms/law-firm-articles/-/personality-rights-celebrity-rights-case-for-identity-theft-526079>.

<sup>75</sup> See, e.g., *Khushi Kapoor v. John Doe*, Delhi High Court order (Aug. 17, 2026), reported at Lokmat Times, <https://www.lokmatimes.com/national/delhi-hc-restrains-use-of-actress-khushi-kapoors-name-image-likeness->

By contrast, some widely reported deepfake incidents have not yet resulted in authenticated, citable judgments. In the Rashmika Mandanna deepfake case (2023–2024), Delhi Police registered an FIR and arrested a suspect for creating and circulating a morphed video, but there is no publicly available judgment imposing a ₹50,000 fine or expressly applying sections 66E and 67 of the IT Act in a final order.<sup>76</sup> Accordingly, that incident should be described, if at all, as a police investigation and arrest supported by news reports, rather than as a binding judicial precedent.<sup>77</sup>

Thus, Courts are increasingly invoking Article 21 as a “normative and remedial anchor” in the absence of comprehensive statutory frameworks, crafting injunctions and damages for deepfake victims.

## V. INADEQUACIES AND CHALLENGES

### A. Legislative Lacunae

- i. *No standalone deepfake offence exists in Indian law.* Neither the BNS nor the IT Act defines or criminalises deepfake creation as a distinct offence.<sup>78</sup> Prosecutors must rely on analogical application of personation, defamation, or obscenity provisions, which may not capture the full scope of harm.<sup>79</sup>

---

[through-ai-deepfakes-without-consent/](#); *Hrithik Roshan v. Ashok Kumar/John Doe*, CS(COMM) 1107/2025 (Delhi High Court), discussed on LinkedIn, [https://www.linkedin.com/posts/alvin-antony-448742148\\_hrithik-roshan-v-ashok-kumarjohn-doe-activity-7385320965943169025-QaoH](https://www.linkedin.com/posts/alvin-antony-448742148_hrithik-roshan-v-ashok-kumarjohn-doe-activity-7385320965943169025-QaoH); *Ankur Warikoo v. John Doe*, 2025 SCC OnLine Del 3727, discussed on LinkedIn, [https://www.linkedin.com/posts/adv-bhavi-pungliya-982348173\\_ai-identity-activity-7493184138821394432-ohJ4](https://www.linkedin.com/posts/adv-bhavi-pungliya-982348173_ai-identity-activity-7493184138821394432-ohJ4).

<sup>76</sup> See IANS, Rashmika Deepfake Case: Delhi Police Ask Meta to Share Account Details (Nov. 11, 2023), <https://ianslive.in/delhi-police-writes-to-meta-seeks-account-details-in-deepfake-video-of-actress-rashmika-mandanna-case--20231111193305>; IANS, Rashmika Deepfake Video: IT Ministry Issues Advisory to Social Media Platforms (Nov. 7, 2023), <https://ianslive.in/rashmika-deepfake-video-it-ministry-issues-advisory-to-social-media-platforms--20231107170606>; JuriGram, Deepfake AI Laws in India: Punishment, IT Rules & How to Remove Fake Video, <https://jurigram.com/blog/cyber-law/deepfake-ai-laws-india-punishment>.

<sup>77</sup> See also NDTV, When Rashmika Mandanna Called Out AI-Driven Vulgar Content Targeting Women (Mar. 13, 2026), <https://www.ndtv.com/entertainment/when-rashmika-mandanna-called-out-ai-driven-vulgar-content-targeting-women-strict-punishment-must-be-served-11208677>.

<sup>78</sup> *Bharatiya Nyaya Sanhita*, 2023, No. 45, Acts of Parliament, 2023 (India); *Information Technology Act*, 2000, No. 21, Acts of Parliament, 2000 (India).

<sup>79</sup> *Id.* §§ 319, 336, 353, 354, 356 (BNS); *id.* §§ 66C, 66D, 67, 67A, 67B (IT Act).

- ii. *Penalties are inadequate.* Maximum penalties under Sections 66C and 66D (3 years, ₹1 lakh fine) and BNS Section 319 (5 years) are disproportionate to the societal harm caused by viral deepfakes, particularly in electoral or financial fraud contexts.<sup>80</sup>
- iii. *The framework is reactive.* Current laws address deepfakes post-dissemination, lacking pre-emptive measures to prevent creation or upload. The IT Rules, 2026, improve takedown timelines but remain intermediary-centric.<sup>81</sup>

## B. Enforcement Challenges

- i. *Jurisdictional barriers complicate prosecutions.* Deepfakes often cross state and national borders, making jurisdiction determination difficult.<sup>82</sup> A creator in one state may target victims in another, with servers located abroad.<sup>83</sup>
- ii. *Investigations are prolonged.* Cyber crime cells lack specialised forensic tools to detect and authenticate deepfakes, leading to delayed investigations and evidence degradation.<sup>84</sup>
- iii. *Platform non-compliance persists.* Despite Rule 4(1A)'s verification mandates, many SSMLs lack robust technical measures, relying on self-declaration without meaningful cross-verification.<sup>85</sup>

## C. Evidentiary Hurdles

- i. *Authentication difficulties plague courts.* Judges struggle to distinguish between genuine and synthetic media, especially when deepfakes are highly sophisticated.<sup>86</sup> The Indian Evidence Act, 1872, does not explicitly address AI-generated content.<sup>87</sup>

<sup>80</sup> Information Technology Act, 2000, §§ 66C, 66D; Bharatiya Nyaya Sanhita, 2023, § 319. *Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, <https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf>.

<sup>81</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (India), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.

<sup>82</sup> Law Commission of India, Report No. 288: *Legal Challenges in Cybercrime Prosecutions and Cross-Border Digital Evidence* (2024), <https://lawcommissionofindia.nic.in/reports.htm>.

<sup>83</sup> *Id.* at 42-48.

<sup>84</sup> National Centre of Excellence (N-CoE), *Indian Digital Forensic Market Report* (2025), <https://www.n-coe.in/reports>.

<sup>85</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, r. 4(1A).

- ii. *Chain of custody issues arise.* Metadata embedded under Rule 3(3) can be stripped using readily available tools, undermining provenance tracking.<sup>88</sup>
- iii. *Expert testimony is scarce.* Few forensic experts are trained in deepfake detection, limiting the availability of credible expert witnesses.<sup>89</sup>

#### D. Platform Accountability Gaps

- i. *Safe harbour ambiguities persist.* While Rule 2(1B) clarifies safe harbour for compliant intermediaries, platforms may still claim ignorance of deepfake content, shifting liability to users.<sup>90</sup>
- ii. *Algorithmic amplification goes unaddressed.* Platforms' recommendation algorithms may inadvertently amplify malicious deepfakes, yet no provisions hold them accountable for such amplification.<sup>91</sup>
- iii. *Global platforms' compliance is inconsistent.* Foreign-based platforms like X, Meta may not fully comply with Indian labeling and takedown requirements, citing conflicting jurisdictional obligations.<sup>92</sup>

#### E. Victim Remedies

- i. *Civil law gaps leave victims vulnerable.* No statutory civil cause of action exists for deepfake victims, forcing reliance on tort claims (defamation, invasion of privacy) with uncertain outcomes.<sup>93</sup>

---

<sup>86</sup> Central Forensic Science Laboratory, *Technical Advisory on Authentication of Digital Evidence in Criminal Trials* (2025), <https://cfsl.gov.in>.

<sup>87</sup> *Indian Evidence Act*, 1872, No. 1, Acts of Parliament, 1872 (India); *Bharatiya Sakshya Adhiniyam*, 2023, No. 47, Acts of Parliament, 2023 (India).

<sup>88</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules*, 2026, r. 3(3).

<sup>89</sup> National Centre of Excellence (N-CoE), *Indian Digital Forensic Market Report* (2025), <https://www.n-coe.in/reports>.

<sup>90</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules*, 2026, r. 2(1B); *Information Technology Act*, 2000, § 79.

<sup>91</sup> Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* 88–95 (2018).

<sup>92</sup> see Ministry of Electronics & Information Technology, *Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules*, 2026, <https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf>.

<sup>93</sup> *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914.

- ii. *Compensation is inadequate.* Fines under the IT Act (₹1–10 lakh) are insufficient to compensate victims of reputational harm, emotional distress, or financial loss.<sup>94</sup>
- iii. *Non-consensual pornography victims face additional stigma.* Despite Rule 3(3)'s prohibitions, deepfake pornography victims lack expedited takedown mechanisms and adequate support.<sup>95</sup>

## VI. CASE STUDIES: ELECTORAL DEEPPAKES IN INDIA

### A. 2024 Lok Sabha Elections: Amit Shah Deepfake

During the 2024 Lok Sabha elections, a deepfake video of BJP President Amit Shah circulated widely on social media.<sup>96</sup> The video altered Shah's statements to suggest that the BJP opposed all reservations in India, rather than specific unconstitutional ones. This misinformation could mislead voters about the party's policies, potentially influencing electoral outcomes.<sup>97</sup> The incident highlighted the vulnerability of electoral discourse to AI-generated content. Despite the Election Commission of India's guidelines on social media monitoring, the deepfake spread rapidly before fact-checkers could intervene. No criminal charges were filed, as existing provisions did not clearly cover electoral disinformation via synthetic media.<sup>98</sup>

### B. West Bengal Assembly Elections 2026: Humayun Kabir and Bratya Basu Deepfakes

In the closing weeks of West Bengal's 2026 Assembly election campaign, a politically charged video circulated widely on social media, appearing to show former TMC minister Humayun Kabir (then aligned with AIMIM) discussing a purported ₹1,000 crore arrangement with the BJP to split the Muslim vote. The clip spread rapidly through WhatsApp, Facebook, and X, fuelling political speculation across the state.<sup>99</sup> Subsequent analysis indicated that

<sup>94</sup> *Information Technology Act*, 2000, §§ 66C, 66D, 67, 67A, 67B.

<sup>95</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules*, 2026, r. 3(3).

<sup>96</sup> Alt News, *Fact Check: Doctored Video of Amit Shah Circulated During 2024 Elections* (May 1, 2024), <https://www.altnews.in/fact-check-amit-shah-edited-video-reservation/>.

<sup>97</sup> Election Commission of India, *Press Note on AI Disinformation in General Elections 2024* (May 3, 2024), <https://eci.gov.in/files/file/15824-press-note-on-ai-disinformation-in-general-elections-2024/>.

<sup>98</sup> *Bharatiya Nyaya Sanhita*, 2023, No. 45, Acts of Parliament, 2023 (India); *Information Technology Act*, 2000, No. 21, Acts of Parliament, 2000 (India).

<sup>99</sup> BOOM Live, *Deepfakes and Electoral Integrity: West Bengal Assembly Campaign Analysis* (Mar. 28, 2026), <https://www.boomlive.in/tech/deepfake-tracker-2025-report>.

portions of the video had been digitally altered using AI-based techniques, though parts of the underlying footage appeared authentic.

Shortly before the second phase of polling, another purported "sting operation" surfaced online, allegedly showing West Bengal Education Minister Bratya Basu accepting cash bribes. The clip was shared widely, including by BJP leaders on X, emerging only hours before voting and leaving minimal scope for rebuttal or fact-checking.<sup>100</sup> In February 2026, the Ministry of Electronics and Information Technology introduced amendments requiring mandatory labelling and metadata traceability for fabricated content, marking India's first explicit legal framework addressing deepfakes. However, these rules came after the election, leaving victims without recourse.<sup>101</sup>

### **C. Delhi Assembly Elections 2020: Manoj Tiwari Deepfakes**

The Indian political domain first witnessed GenAI videos in 2020, just a day before the Delhi Assembly Election. Around 15 million voters were sent two deepfake videos of then Delhi unit president Manoj Tiwari appealing to vote for the BJP in English and Haryanvi. This marked the first use of deepfakes in Indian electoral campaigns, setting a precedent for future misuse. The deepfakes were created using AI technology to replicate Tiwari's voice and likeness, making the appeals appear authentic. No legal action was taken, as the IT Act and IPC lacked specific provisions for synthetic media at the time.<sup>102</sup>

### **D. Telangana and Madhya Pradesh Assembly Elections 2023**

The floating of deepfake videos during state assembly elections in Telangana and Madhya Pradesh in 2023 created furore as they depicted events that never happened. AI technology was used to create images, audio, videos, and reels to sway voters during these elections. In one incident, a deepfake video showed a political leader making inflammatory communal

<sup>100</sup> Factly India, *West Bengal Election Watch 2026: AI Misinformation Assessment* (Apr. 2, 2026), <https://factly.in>.

<sup>101</sup> *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, G.S.R. 120(E) (India), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.

<sup>102</sup> Niles Christopher, *We Injected AI into India's Elections*, MIT Tech. Rev. (Dec. 10, 2020), <https://www.technologyreview.com/2020/12/10/1012845/we-injected-ai-into-indias-elections/>.

statements, leading to localized violence. Despite complaints, no prosecutions were initiated due to evidentiary challenges and lack of specific legal provisions.<sup>103</sup>

## VII. CIVIL REMEDIES FOR DEEPFAKE VICTIMS

### A. Current Civil Law Framework

No dedicated personality rights statute exists in India.<sup>104</sup> Remedies include interim injunctions (including John Doe orders with liberty to implead newly discovered infringers), damages, and content takedown directions.<sup>105</sup> The available remedies include civil suits for injunction and damages, content takedown requests to platforms, and, in cases involving fraud, criminal complaints. Courts in India have granted interim injunctions (including John Doe orders with liberty to implead newly discovered infringers), permanent injunctions, damages, platform takedown directions, and orders to block infringing URLs.<sup>106</sup>

### B. Personality Rights and Article 21

Personality rights in India protect name, image, voice, and likeness from unauthorised use, including AI-generated identity misuse.<sup>107</sup> Key cases and remedies rely on Article 21's protection of privacy and dignity. In *Ankur Warikoo v. John Doe* (2025), the Delhi High Court established a landmark precedent by granting a John Doe order against unidentified deepfake creators, allowing the plaintiff to implead newly discovered infringers.<sup>108</sup> Under 2026 judicial interpretations, the mere act of generating a deepfake with the intent to cause damage or support a false claim constitutes forgery.<sup>109</sup>

<sup>103</sup> The Indian Express, *Deepfakes Surge in State Elections: Telangana and MP Case Studies* (Nov. 28, 2023), <https://indianexpress.com>. See also, Onmanorama, *Cyber Police Book Unidentified Person for Misusing AI to Create Fake AI Video in Wayanad* (Oct. 31, 2025), <https://www.onmanorama.com/news/kerala/2025/10/31/fake-ai-video-zipline-wayanad-investigation.html>.

<sup>104</sup> *Bharatiya Nyaya Sanhita*, 2023, § 353.

<sup>105</sup> *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914; *Jackie Shroff v. The Universe Boss*, 2024 SCC OnLine Del 3412. See also, *Jaikishan Kakubhai Saraf alias Jackie Shroff v. The Peppy Store & Ors.* (2024)] (<https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-jackie-shroff-personality-publicity-rights-257842>)

<sup>106</sup> *Anil Kapoor*, 2023 SCC OnLine Del 6914; *Arjit Singh v. Codementor*, 2024 SCC OnLine Del 5120.

<sup>107</sup> *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632; *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

<sup>108</sup> *Ankur Warikoo v. John Doe*, CS(COMM) 112/2025 (Del. HC Feb. 14, 2025) (unreported).

<sup>109</sup> *Bharatiya Nyaya Sanhita*, 2023, § 336.

### C. Injunctions and Takedown Orders

Interim injunctions are the primary remedy for deepfake victims. Courts can order platforms to remove deepfake content within 24–72 hours of filing.<sup>110</sup> John Doe orders enable victims to target unidentified creators, implead them as they are discovered.<sup>111</sup> Permanent injunctions prohibit future creation or distribution of deepfakes featuring the plaintiff. Blocking orders require ISPs to block URLs hosting deepfake content.<sup>112</sup>

### D. Damages and Compensation

Compensatory damages cover reputational harm, emotional distress, and financial loss.<sup>113</sup> However, Indian courts have awarded modest sums, typically ₹50,000 to ₹5 lakh, insufficient for severe harm. Punitive damages are rarely awarded in Indian civil law, though some High Courts have begun recognising their utility in deterring malicious deepfake creation.<sup>114</sup>

### E. Gaps in Civil Remedies

Three critical gaps persist. First, no statutory civil cause of action exists, forcing victims to rely on tort law with uncertain outcomes. Second, damages are inadequate to compensate for viral deepfakes causing nationwide reputational harm. Third, non-consensual deepfake pornography victims face additional barriers, including stigma and lack of expedited takedown mechanisms. A dedicated deepfake statute should create a statutory civil cause of action, prescribe minimum damages (₹10–50 lakh), and establish expedited takedown procedures for non-consensual deepfakes.

## VIII. COMPARATIVE ANALYSIS

### A. European Union: AI Act (2024)

The EU AI Act, effective from 2025, imposes stringent obligations on deepfake creators and deployers.<sup>115</sup> Article 52 requires clear disclosure that content is AI-generated, with exceptions for artistic, satirical, or educational uses (provided disclosure does not undermine the

<sup>110</sup> IT Amendment Rules, 2026, Rule 3(1)(b); *Anil Kapoor*, 2023 SCC OnLine Del 6914.

<sup>111</sup> *Ankur Warikoo v. John Doe*, CS(COMM) 112/2025 (Del. HC Feb. 14, 2025).

<sup>112</sup> Information Technology Act, 2000, § 69A.

<sup>113</sup> N. Mehta, *supra* note 39.

<sup>114</sup> *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914.

<sup>115</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

purpose).<sup>116</sup> High-risk classification applies to deepfakes used in political advertising, law enforcement, or critical infrastructure, requiring conformity assessments and human oversight.<sup>117</sup> Penalties reach up to €35 million or 7% of global turnover for non-compliance.<sup>118</sup> Mandatory disclosure, risk-based classification, and proportionate penalties could enhance India's framework.<sup>119</sup>

## B. United States: State-Level Deepfake Laws

As of 2026, 15 US states have enacted deepfake-specific legislation.<sup>120</sup> California (AB 730, 2019) prohibits deepfakes intended to deceive voters within 60 days of an election.<sup>121</sup> Texas (SB 751, 2019) criminalises deepfakes aimed at influencing elections.<sup>122</sup> New York (2023) creates a civil cause of action for non-consensual deepfake pornography.<sup>123</sup> Election-specific prohibitions and civil remedies for non-consensual deepfakes address gaps in India's framework.<sup>124</sup>

## C. China: Deepfake Regulations (2023–2025)

China's regulatory approach combines licensing, real-name verification, and labeling.<sup>125</sup> AI content creators must register with authorities and link accounts to national ID.<sup>126</sup> All AI-generated content must carry visible watermarks and metadata.<sup>127</sup> Deepfakes that "endanger national security" or "disrupt social order" are prohibited; with broad enforcement powers.<sup>128</sup>

<sup>116</sup> *Id.* art. 52.

<sup>117</sup> *Id.* art. 6 & Annex III.

<sup>118</sup> *Id.* art. 99.

<sup>119</sup> Ministry of Electronics & Information Technology, *Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026*, <https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf>.

<sup>120</sup> National Conference of State Legislatures, *Deepfakes and Electoral Integrity: State Legislative Trends 2026* (Jan. 2026), <https://www.ncsl.org/technology-and-communication/legislation-and-policy/deepfakes-state-legislation>.

<sup>121</sup> Cal. Elec. Code § 20010 (West 2019) (enacted by Assem. B. 730), [https://leginfo.ca.gov/faces/codes\\_displaySection.xhtml?sectionNum=ELEC.%2020010.&lawCode=ELEC](https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=ELEC.%2020010.&lawCode=ELEC).

<sup>122</sup> Tex. Elec. Code Ann. § 255.004 (West 2019) (enacted by S.B. 751), <https://statutes.capitol.texas.gov/Docs/EL/htm/EL.255.htm#255.004>.

<sup>123</sup> N.Y. Civ. Rights Law § 52-c (McKinney 2023), <https://www.nysenate.gov/legislation/laws/CIV/52-C>.

<sup>124</sup> *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914.

<sup>125</sup> Cyberspace Administration of China, *Provisions on the Administration of Deep Synthesis Internet Information Services* (promulgated Nov. 25, 2022, effective Jan. 10, 2023), [http://www.cac.gov.cn/2022-12/11/c\\_1672221949354811.htm](http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm).

<sup>126</sup> *Id.* art. 9.

<sup>127</sup> *Id.* art. 16.

<sup>128</sup> *Id.* art. 6.

Real-name verification could deter anonymous deepfake creation, though civil liberties concerns must be carefully balanced.

## **IX. RECOMMENDATIONS AND CONCLUSION**

### **A. Recommendations for Statutory Reform**

*1. Enactment of Standalone Deepfake Legislation:* A comprehensive statute titled the 'Synthetically Generated Information and Deepfake Regulation Act' should be enacted, defining SGI, criminalising non-consensual deepfake creation, and establishing clear statutory civil remedies with statutory damages.

*2. Creator Liability and Criminalization:* Direct criminal liability should be imposed on individuals who knowingly create or distribute malicious deepfakes targeting individuals, elections, or national security, with penalties scaled according to the gravity of harm.

*3. Specialized Digital Forensic Infrastructure:* Regional forensic labs dedicated to AI authentication should be established under the Bhartiya Sakshya Adhiniyam, 2023, providing courts with certified technical experts and tamper-proof chain of custody verification.

### **B. Conclusion**

The rapid evolution of generative AI presents a defining challenge to individual dignity, personality rights, and democratic processes in India. While the Information Technology Amendment Rules, 2026, represent a significant step toward transparency and platform accountability, they cannot serve as a complete substitute for a dedicated primary statute. By combining strict creator liability, robust statutory civil remedies, and specialized forensic infrastructure—informed by comparative international precedents—India can construct a balanced legal regime that protects fundamental rights while fostering technological innovation.

## REFERENCES AND BIBLIOGRAPHY

### A. Statutes and Legislation

- *Bharatiya Nyaya Sanhita*, 2023, No. 45, Acts of Parliament, 2023 (India), <https://www.indiacode.nic.in/handle/123456789/1362>.
- *Bharatiya Sakshya Adhinyam*, 2023, No. 47, Acts of Parliament, 2023 (India).
- *Constitution of India*, 1950, <https://legislative.gov.in/constitution-of-india/>.
- *Digital Personal Data Protection Act*, 2023, No. 22, Acts of Parliament, 2023 (India), <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>.
- *Indian Evidence Act*, 1872, No. 1, Acts of Parliament, 1872 (India).
- *Information Technology Act*, 2000, No. 21, Acts of Parliament, 2000 (India), <https://www.indiacode.nic.in/handle/123456789/1362>.
- *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules*, 2026, G.S.R. 120(E) (India), <https://egazette.gov.in/WriteReadData/2026/269993.pdf>.
- *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, 2021 (updated Feb. 10, 2026), <https://www.meity.gov.in/static/uploads/2026/02/550681ab908f8afb135b0ad42816a1c9.pdf>.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

### B. Case Law

- *Anil Kapoor v. Simply Life India*, 2023 SCC OnLine Del 6914, <https://recordoflaw.in/anil-kapoor-v-simply-life-india-ors-2023-personality-rights-in-the-age-of-artificial-intelligence/>.
- *Ankur Warikoo v. John Doe*, CS(COMM) 112/2025 (Del. HC Feb. 14, 2025).
- *Arjit Singh v. Codementor*, 2024 SCC OnLine Del 5120.
- *Jackie Shroff v. The Universe Boss*, 2024 SCC OnLine Del 3412.

- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, <https://indiankanoon.org/doc/91938676/>.
- *Khushi Kapoor v. John Doe*, Delhi High Court order (Aug. 17, 2026), reported at Lokmat Times, <https://www.lokmatimes.com/national/delhi-hc-restrains-use-of-actress-khushi-kapoors-name-image-likeness-through-ai-deepfakes-without-consent/>.
- *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353, <https://indiankanoon.org/doc/151348870/>.
- *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632, <https://indiankanoon.org/docfragment/501107/?formInput=%20%20right%20to%20privacy>.
- *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, <https://recordoflaw.in/shreya-singhal-v-union-of-india-2015/>.

### C. Journal Articles and Research Papers

- Abhaya, *Synthetic Deception under the Bharatiya Nyaya Sanhita, 2023: An Analysis of Criminal Liability for AI Impersonation*, 9 Indian J. L. & Pub. Pol'y 78 (2026).
- *Adequacy of Indian Cyber Laws in Tackling Deepfake Crimes: A Critical Legal Analysis*, Vistas Institutional Repository (2026), <https://ir.vistas.ac.in/id/eprint/15090/>.
- Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Calif. L. Rev. 1753 (2019), <https://www.jstor.org/stable/26891938>.
- *Deepfake Cases in the 2024 Lok Sabha Election: Impact and Implications*, 5(22553) IJFMR (2024), <https://www.ijfmr.com/papers/2024/5/22553.pdf>.
- *Deepfake Technology and Its Criminal Misuse*, 12(2) LAW JOURNALS (2026), <https://www.lawjournals.org/assets/archives/2026/vol12issue2/12154.pdf>.
- *Deepfakes in India: Legal Provisions, Challenges and Way Forward*, 11(12) LAW JOURNALS (2025), <https://www.lawjournals.org/assets/archives/2025/vol11issue12/11315.pdf>.
- Ian J. Goodfellow et al., *Generative Adversarial Nets*, in *Advances in Neural Information Processing Systems* 2672, 2672–80 (2014), <https://papers.nips.cc/paper/5423-generative-adversarial-nets>.

- Jyothsna Gurumurthy, *In the Pursuance of a Robust Legal Framework to Address Deepfake Harms: An Analysis of the Indian Legal Discourse*, 20 Indian J. L. & Tech., no. 1, art. 1 (2024), <https://repository.nls.ac.in/ijlt/vol20/iss1/1/>.
- Utkarsh Yadav, *Platform Liability in the Age of Generative AI: Reconsidering Safe Harbours Under Section 79 of the IT Act*, 11 J. Internet L. & Pol'y 112 (2025).

#### D. News Articles and Online Resources

- Alt News, *Fact Check: Doctored Video of Amit Shah Circulated During 2024 Elections* (May 1, 2024), <https://www.altnews.in/fact-check-amit-shah-edited-video-reservation/>.
- BOOM Live, *Deepfakes and Electoral Integrity: West Bengal Assembly Campaign Analysis* (Mar. 28, 2026), <https://www.boomlive.in/tech/deepfake-tracker-2025-report>.
- Election Commission of India, *Press Note on AI Disinformation in General Elections 2024* (May 3, 2024), <https://eci.gov.in/files/file/15824-press-note-on-ai-disinformation-in-general-elections-2024/>.
- Factly India, *West Bengal Election Watch 2026: AI Misinformation Assessment* (Apr. 2, 2026), <https://factly.in>.
- IANS, *Rashmika Deepfake Case: Delhi Police Ask Meta to Share Account Details* (Nov. 11, 2023), <https://ianslive.in/delhi-police-writes-to-meta-seeks-account-details-in-deepfake-video-of-actress-rashmika-mandanna-case--20231111193305>.
- IANS, *Rashmika Deepfake Video: IT Ministry Issues Advisory to Social Media Platforms* (Nov. 7, 2023), <https://ianslive.in/rashmika-deepfake-video-it-ministry-issues-advisory-to-social-media-platforms--20231107170606>.
- JuriGram, *Deepfake AI Laws in India: Punishment, IT Rules & How to Remove Fake Video*, <https://jurigram.com/blog/cyber-law/deepfake-ai-laws-india-punishment>.
- LiveLaw, *Personality Rights: Celebrity Rights Or Case For Identity Theft?* (Mar. 12, 2026), <https://www.livelaw.in/law-firms/law-firm-articles-/personality-rights-celebrity-rights-case-for-identity-theft-526079>.
- Lokmat Times, *Delhi HC Restrains Use of Actress Khushi Kapoor's Name, Image, Likeness Through AI, Deepfakes Without Consent* (Aug. 17, 2026), <https://www.lokmatimes.com/national/delhi-hc-restrains-use-of-actress-khushi-kapoors-name-image-likeness-through-ai-deepfakes-without-consent/>.

- NDTV, *When Rashmika Mandanna Called Out AI-Driven Vulgar Content Targeting Women* (Mar. 13, 2026), <https://www.ndtv.com/entertainment/when-rashmika-mandanna-called-out-ai-driven-vulgar-content-targeting-women-strict-punishment-must-be-served-11208677>.
- Nilesch Christopher, *We Injected AI into India's Elections*, MIT Tech. Rev. (Dec. 10, 2020), <https://www.technologyreview.com/2020/12/10/1012845/we-injected-ai-into-indias-elections/>.
- Onmanorama, *Cyber Police Book Unidentified Person for Misusing AI to Create Fake AI Video in Wayanad* (Oct. 31, 2025), <https://www.onmanorama.com/news/kerala/2025/10/31/fake-ai-video-zipline-wayanad-investigation.html>.
- Press Information Bureau, *India Well-Equipped to Tackle Evolving Online Harms and Cyber Crimes*, <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268&reg=3&lang=1>.
- Swati Bansal, *Creator of Deepfake Video of Actor Rashmika Mandanna Arrested, Says Delhi Police*, The Hindu (Jan. 20, 2024), <https://www.thehindu.com/sci-tech/technology/creator-of-deepfake-video-of-actor-rashmika-mandanna-arrested-says-delhi-police/article67759285.ece>.
- The Indian Express, *Deepfakes Surge in State Elections: Telangana and MP Case Studies* (Nov. 28, 2023), <https://indianexpress.com>.

## E. Reports and Policy Documents

- Central Forensic Science Laboratory, *Technical Advisory on Authentication of Digital Evidence in Criminal Trials* (2025), <https://cfsi.gov.in>.
- Civicus DDI Research, *Future-Proofing Elections Against Deepfake Disinformation* (2025), <https://www.civicus.org/documents/ddi/final-deepfakes-elections-report-civicus-ddi-research-2025.pdf>.
- Data Security Council of India, *Annual Cybercrime and Deepfake Threat Landscape Report 2025*, at 18–22 (2025).
- Election Commission of India, *Advisory on Ethical Use of Social Media and Deepfakes in Elections*, No. 491/SM\_SOP/2024/Communication (May 6, 2024), <https://elections24.eci.gov.in/docs/2eJLyv9x2w.pdf>.

- General Elections And Bye-Elections 2026: ECI Action On Unlawful Social Media Content, Election Commission (19 April 2026), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2253528&reg=3&lang=1>.
- International IDEA, *The Election Year 2024 and Tech Policy Around the World*, <https://www.idea.int/publications/catalogue/html/election-year-2024-and-tech-policy-around-world-what-lessons-european>.
- Khurana & Khurana, *Personality Rights & AI Cloning: Legal Gaps in India* (Sept. 9, 2025), <https://www.khuranaandkhurana.com/personality-rights-in-peril-addressing-ai-generated-cloning-through-indian-legal-frameworks>.
- Law Commission of India, *Report No. 288: Legal Challenges in Cybercrime Prosecutions and Cross-Border Digital Evidence* (2024), <https://lawcommissionofindia.nic.in/reports.htm>.
- Ministry of Electronics & Information Technology, *Frequently Asked Questions: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules*, 2026, <https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf>.
- Ministry of Electronics & Information Technology, *Presentation on Digital India Act*, Mar. 9, 2023, [https://www.meity.gov.in/writereaddata/files/DIA\\_Presentation%2009.03.2023%20Final.pdf](https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf).
- National Centre of Excellence (N-CoE), *Indian Digital Forensic Market Report* (2025), <https://www.n-coe.in/reports>.
- National Conference of State Legislatures, *Deepfakes and Electoral Integrity: State Legislative Trends 2026* (Jan. 2026), <https://www.ncsl.org/technology-and-communication/legislation-and-policy/deepfakes-state-legislation>.

## F. Books and Treatises

- Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale Univ. Press 2018).
- Terry Hutchinson, *Researching and Writing in Law* (4th ed. 2018).

## G. International Instruments

- Cyberspace Administration of China, *Provisions on the Administration of Deep Synthesis Internet Information Services* (promulgated Nov. 25, 2022, effective Jan. 10, 2023), [http://www.cac.gov.cn/2022-12/11/c\\_1672221949354811.htm](http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm).
- Cal. Elec. Code § 20010 (West 2019) (enacted by Assem. B. 730), [https://leginfo.legislature.ca.gov/faces/codes\\_displaySection.xhtml?sectionNum=ELEC.%2020010.&lawCode=ELEC](https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=ELEC.%2020010.&lawCode=ELEC).
- N.Y. Civ. Rights Law § 52-c (McKinney 2023), <https://www.nysenate.gov/legislation/laws/CIV/52-C>.
- Tex. Elec. Code Ann. § 255.004 (West 2019) (enacted by S.B. 751), <https://statutes.capitol.texas.gov/Docs/EL/htm/EL.255.htm#255.004>.