

---

# DEEPFAKES AND CYBERCRIME IN INDIA: REASSESSING INTERMEDIARY LIABILITY, DIGITAL EVIDENCE AND VICTIM PROTECTION IN THE EMERGING SYNTHETIC MEDIA REGIME

---

Srushti Choche, D.E.S. Shri Navalmal Firodiya Law College, Pune

## ABSTRACT

Deepfake technology has altered the relationship between artificial intelligence, identity and digital communication. Unlike ordinary manipulated media, sophisticated synthetic audiovisual material can reproduce a person's face, voice, mannerisms or apparent statements with a degree of realism capable of producing fraud, reputational injury, non-consensual sexual imagery, impersonation and political misinformation. Indian law has historically addressed these harms through provisions directed at the underlying conduct rather than through a dedicated deepfake offence. The regulatory position has, however, begun to change. The 2026 amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduced specific due-diligence requirements concerning synthetically generated information ("SGI"), including identification, labelling and technical verification obligations for significant social media intermediaries. This paper argues that the principal contemporary question is therefore not simply whether India needs a separate deepfake statute, but whether the emerging regulatory architecture allocates responsibility effectively across creators, AI-service providers, intermediaries and the State. The study adopts a doctrinal, analytical and comparative methodology and develops a "deepfake accountability chain" comprising creation, dissemination, detection, attribution, evidentiary verification and remedy. It further examines the impact of synthetic media on electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023, and the growing judicial use of personality-rights and injunctionbased remedies. The paper concludes that labelling and intermediary regulation are useful but cannot independently solve attribution, authenticity or victim-remedy problems. India requires a coordinated, rights-based model combining provenance mechanisms, clear responsibility, specialised forensic procedures, rapid victim remedies and safeguards for legitimate expression.

**Keywords:** Artificial Intelligence; Cybercrime; Deepfakes; Digital Evidence; Intermediary Liability; Privacy; Synthetic Media; Victim Protection.

## INTRODUCTION

The rapid development of generative artificial intelligence has transformed digital manipulation from a specialist editing practice into a widely accessible form of synthetic media. Deepfakes are particularly significant because they can make a person appear to speak, act or endorse something that never occurred. The resulting harm is not confined to misinformation. A synthetic representation can be used as an instrument of impersonation, fraud, sexual abuse, reputational attack or identity appropriation. The legal difficulty arises because the same technological process can support lawful creative expression and unlawful conduct, making regulation dependent upon context, intent, harm and the means through which the material is distributed.<sup>1</sup>

Indian regulation initially approached deepfake-related misconduct indirectly. The **Information Technology Act, 2000**, the Information Technology Rules, 2021 and the general criminal law could be applied when synthetic media satisfied the ingredients of an existing offence. The enactment of the **Bharatiya Nyaya Sanhita, 2023** and **Bharatiya Sakshya Adhiniyam, 2023** also changed the surrounding criminal and evidentiary framework. More recently, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 introduced a specific regulatory framework for synthetically generated information. This development makes it necessary to reassess the earlier assumption that Indian law is simply characterised by the absence of deepfake-specific regulation.<sup>2</sup>

The central argument of this paper is that the regulatory challenge has moved from a question of legislative absence to one of responsibility allocation. A harmful deepfake may involve a creator, an AI-generation service, an intermediary, a social-media platform, an investigator, a forensic expert and a court. Each actor controls a different part of the information chain. A legally effective response must therefore address not only whether the creator can be prosecuted but also how synthetic content is identified, how evidence is preserved and authenticated, how platforms respond to complaints, and how victims obtain effective relief.

---

<sup>1</sup> Danielle Keats Citron & Bobby Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753, 1758–64 (2019).

<sup>2</sup> Ministry of Electronics & Information Technology, Government of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026).

This paper develops that approach through a “deepfake accountability chain.”

The study is guided by five research questions: (1) how has Indian regulation moved from general cybercrime provisions towards governance of synthetically generated information; (2) how should responsibility be distributed among creators, AI services and intermediaries; (3) whether provenance and labelling mechanisms improve the reliability of synthetic-media evidence; (4) whether existing removal and victim-remedy mechanisms are adequate; and (5) how can harmful deepfakes be regulated without disproportionately restricting legitimate expression? The paper uses doctrinal, analytical and comparative legal research, relying principally upon legislation, rules, government materials, judicial decisions and established academic literature. No primary survey data is claimed or generated.

## CONCEPTUALISING DEEPFAKES AS DIGITAL IDENTITY HARM

A deepfake is best understood functionally rather than merely as a particular software technique. It refers to synthetic or materially manipulated audio-visual content produced through computational methods in a manner that can appear authentic or depict a real person in a fabricated situation. Face replacement, voice cloning, lip synchronisation and synthetic video generation are different technical forms, but their common legal characteristic is the capacity to create a misleading representation of identity or events. This functional approach is preferable for law because technical methods change faster than statutory definitions.<sup>3</sup>

Deepfake technology is not inherently unlawful. Synthetic media may be used for filmmaking, dubbing, education, accessibility, historical reconstruction, satire and artistic experimentation. The legal wrong emerges when the technology is connected to conduct that infringes another person's rights or violates criminal law. A synthetic video of a fictional character is fundamentally different from a fabricated video that falsely attributes a criminal confession to an identifiable person. Regulation should consequently focus on harmful uses and measurable risks rather than treating every synthetic representation as prohibited.<sup>4</sup>

The distinctive harm of deepfakes lies in the combination of identity appropriation and evidentiary ambiguity. A manipulated recording may injure the person depicted, but it can also

---

<sup>3</sup> Matthew Groh et al., Deepfake Detection by Human Crowds, Machines, and Machine-Machine Collaboration, 118 Proc. Nat'l Acad. Sci. 1 (2021).

<sup>4</sup> Citron & Chesney, *supra* note 1, at 1758–84.

affect the evidentiary environment in which genuine recordings are evaluated. Once the public knows that realistic media can be fabricated, an accused person may attempt to dismiss authentic evidence as synthetic. This phenomenon, often described as the “liar’s dividend,” creates a broader institutional problem for journalism, courts, elections and public accountability.<sup>5</sup>

Deepfake harm can therefore be divided into at least four overlapping categories: identity and financial deception; sexualised and gender-based abuse; reputational and personality-rights injury; and public-interest harms such as misinformation. The categories are analytically useful because different harms call for different legal responses. Fraud may require attribution and financial investigation; non-consensual intimate deepfakes require urgent removal and confidentiality; personality-rights cases may require injunctions; and political misinformation raises heightened concerns about speech and democratic participation.

## FROM FRAGMENTED LIABILITY TO SYNTHETIC-MEDIA GOVERNANCE

The **Information Technology Act, 2000** remains an important statutory foundation. Sections **66C** and **66D** may become relevant where electronic identity features or computer resources are used for identity theft or cheating by personation. **Sections 67, 67A and 67B** may apply to obscene, sexually explicit or child sexual-abuse material in electronic form. **Section 67C** concerns preservation and retention of information by intermediaries, while **section 79** forms part of the statutory framework governing intermediary safe harbour. The Act, however, was enacted long before contemporary generative AI and therefore regulates the consequences or manner of misuse rather than the technology as such.<sup>6</sup>

The **Bharatiya Nyaya Sanhita, 2023** supplements this framework through offences including cheating, cheating by personation and defamation. A deepfake does not automatically constitute one of these offences merely because it is synthetic. The prosecution must establish the elements of the particular offence. This is both a strength and a limitation of technology-neutral criminal law: the provisions can remain relevant when technology changes, but they may leave some forms of synthetic-media harm insufficiently captured where no existing

---

<sup>5</sup> Id. at 1776–84.

<sup>6</sup> Information Technology Act, No. 21 of 2000, §§ 66C–66D, 67–67C, 79 (India).

offence fits the conduct.<sup>7</sup>

The **Information Technology Rules, 2021** have become increasingly significant because most deepfake harms are amplified through intermediaries. The 2026 amendments now define and regulate synthetically generated information and strengthen due-diligence obligations. Among other things, the amended framework requires measures relating to unlawful SGI and introduces identification, labelling and metadata-related obligations for permissible SGI. Significant social media intermediaries are also required to obtain user declarations concerning whether information is synthetically generated and deploy appropriate technical measures to verify such declarations before publication.<sup>8</sup>

The 2026 amendments represent an important regulatory shift. The State is no longer relying exclusively upon ex post criminal prosecution of an unknown creator. Instead, the regulatory system increasingly places preventive duties upon platforms that control distribution. This may improve the speed of intervention, but it also creates difficult questions about automated verification, false positives, platform discretion and freedom of expression. The effectiveness of the new framework should therefore be measured not simply by the existence of labelling duties but by whether those duties produce reliable provenance, meaningful accountability and proportionate intervention.<sup>9</sup>

The **Digital Personal Data Protection Act, 2023** is relevant where personal data such as facial images, photographs or voice-related information is processed. Its principal function, however, is regulation of digital personal-data processing rather than creation of a comprehensive deepfake offence. It should therefore be treated as complementary to, rather than a substitute for, criminal, intermediary and civil remedies.<sup>10</sup>

## THE DEEPAKE ACCOUNTABILITY CHAIN

The principal analytical contribution of this paper is the proposed deepfake accountability chain: creation, dissemination, detection, attribution, evidentiary verification and remedy. This

---

<sup>7</sup> Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318–19, 356 (India).

<sup>8</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), rr. 3(3), 4(1A) (India).

<sup>9</sup> Ministry of Electronics & Information Technology, Government of India, Section I: Overview and Objectives, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (2026).

<sup>10</sup> Digital Personal Data Protection Act, No. 22 of 2023, §§ 2–8 (India).

model recognises that responsibility is distributed across the digital ecosystem. A criminal-law response focused only on the anonymous creator may fail where the creator cannot be identified, while a platform-only model may impose excessive responsibility on intermediaries for content over which they have limited prior knowledge. The appropriate question is therefore what duty each actor can reasonably perform at each stage of the chain.

At the creation stage, liability should ordinarily turn on the unlawful purpose or foreseeable harmful use rather than the mere technical act of generation. An AI tool may have legitimate applications and cannot sensibly be treated as criminal merely because it is capable of producing deceptive media. Where a creator intentionally fabricates content to impersonate a person, commit fraud, facilitate sexual abuse or cause another legally recognised injury, existing criminal provisions may apply. A future framework should preserve this conduct-based principle while creating clearer rules for especially harmful categories.

At the service-provider stage, the regulatory issue is different. Providers that facilitate generation may not possess the same knowledge or control as the person who commissions the content. Nevertheless, transparency, safety-by-design, provenance support and mechanisms for responding to lawful requests can reduce systemic risk. A proportionate framework should distinguish between general-purpose AI services; specialised impersonation tools and platforms whose principal function is the distribution of synthetic media. A uniform standard for all providers would risk both under-regulation and over-regulation.

At the intermediary stage, the 2026 amendments are particularly significant. Platforms can influence whether content is labelled, how rapidly complaints are processed and whether prohibited material continues to circulate. The legal challenge is to create incentives for effective intervention without turning platforms into private arbiters of lawful political, artistic or journalistic expression. Procedural safeguards, transparent standards and opportunities for review are therefore as important as takedown duties.

Attribution remains the weakest link in many deepfake investigations. Creators may use pseudonymous accounts, disposable identifiers, foreign services or multiple platforms. A technically sophisticated regulatory system cannot produce accountability if investigators cannot connect the content to a person. This makes preservation of platform records, subscriber information, IP-related data and relevant metadata important. It also makes cross-border cooperation and timely preservation requests essential.

The accountability chain therefore suggests a layered model rather than a single-offender model. Creators bear responsibility for unlawful conduct; AI providers may bear defined transparency and safety obligations; intermediaries bear due-diligence and response obligations; investigators must preserve and authenticate evidence; and courts must distinguish the existence of a digital file from the truth of what it depicts. This distribution is more adaptable than a technology-specific criminal offence alone.

## DEEPPAKES AND THE LAW OF DIGITAL EVIDENCE

Synthetic media creates an evidentiary problem that is different from ordinary electronic-record disputes. The question is not only whether a file exists, but whether the file accurately represents the event, person or statement it purports to depict. The **Bharatiya Sakshya Adhiniyam, 2023** recognises the legal status of electronic or digital records subject to the statutory conditions governing electronic evidence. **Sections 61 to 63** are consequently important when a video, audio recording, platform record or forensic output is relied upon in court.<sup>11</sup>

A deepfake case may require evidence concerning the source device, original file, metadata, timestamps, hash values, platform records, account information, chain of custody and expert examination. These elements do not establish truth automatically; rather, they help the court assess authenticity and provenance. The legal system should avoid the assumption that visual realism equals evidentiary reliability. A sophisticated fake can look genuine, while a genuine recording may have been compressed, edited for technical reasons or transferred across platforms without losing its essential authenticity.

The evidentiary challenge is therefore partly technological and partly institutional. Detection tools themselves may produce false positives or become less reliable as generative systems evolve. Courts should not treat an automated “deepfake detector” as conclusive proof. Instead, expert evidence should explain the methodology, limitations, source material and degree of confidence, while the opposing party should have a meaningful opportunity to challenge the technical basis of the conclusion. Judicial competence in digital evidence will consequently become as important as the availability of detection technology.<sup>12</sup>

---

<sup>11</sup> Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63 (India).

<sup>12</sup> See Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63 (India); Matthew Groh et al., *supra* note 3

The problem also extends to preservation. A harmful deepfake may be deleted after a complaint, but deletion can destroy information needed to identify the creator. Conversely, indiscriminate retention of personal data may create privacy risks. A balanced system should preserve evidence that is reasonably necessary for investigation, subject to lawful process, security safeguards and retention limits. The objective should be evidentiary integrity rather than unlimited data collection.

## VICTIM PROTECTION, PERSONALITY RIGHTS AND RAPID REMEDIES

Deepfake victims frequently require a remedy before a criminal trial can occur. The harm may be continuing while the content remains online, and each re-upload can recreate the injury. This is particularly serious in non-consensual intimate deepfake cases, where the victim's identity may be exposed to a large audience and the material may be copied across services. A criminal prosecution that takes years cannot by itself provide an adequate immediate remedy.<sup>13</sup>

The constitutional protection of privacy under **Article 21** provides an important normative basis for addressing identity appropriation. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a constitutionally protected right connected with dignity and autonomy. Deepfake misuse of a person's face, voice or intimate identity may therefore implicate interests beyond conventional property or reputation. The constitutional analysis, however, must be balanced against freedom of expression where synthetic media is used for legitimate commentary, satire, art or journalism.<sup>14</sup>

Indian courts have increasingly used personality-rights and injunction-based remedies in cases involving AI-generated impersonation. In *Ravi Shankar v. John Doe/Ashok Kumar*, the Delhi High Court considered fabricated videos using the plaintiff's name, voice, facial expressions, persona and likeness and granted interim protection against such misuse. The order also directed platform-level removal and provided a mechanism for addressing subsequently discovered infringing material. The decision illustrates the practical value of civil injunctions where unknown creators and rapidly circulating content make conventional litigation inadequate.<sup>15</sup>

---

<sup>13</sup> Information Technology Act, No. 21 of 2000, §§ 67, 67A (India).

<sup>14</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

<sup>15</sup> Ravi Shankar v. John Doe(s)/Ashok Kumar(s) & Ors., CS(COMM) 889/2025, Order (Delhi H.C. Aug. 26, 2025).

The 2026 decision in *Dr. Aniruddha Dhairyadhar Joshi v. John Does/Ashok Kumars* further illustrates the developing judicial response. The Delhi High Court directed platforms to remove or disable identified infringing material and required disclosure of available basic subscriber information in specified circumstances. Such orders show that courts are increasingly addressing deepfakes through a combination of personality rights, intermediary directions and information-disclosure mechanisms.<sup>16</sup>

*Raghav Chadha v. Ashok Kumar/John Doe & Ors.* demonstrates another dimension of the problem. The Delhi High Court recognised that harmful AI-generated material may implicate dignity while also acknowledging that AI is increasingly used as a means of expression, particularly in political contexts. The court's reasoning highlights the constitutional need to balance protection against harmful deepfakes with freedom of speech. This balance should inform statutory and platform-level regulation as well.<sup>17</sup>

A victim-centred framework should therefore provide at least four forms of protection: an accessible complaint mechanism; rapid removal or disabling of unlawful material; preservation of relevant evidence for investigation; and safeguards against repeat dissemination. For intimate or highly sensitive material, confidentiality and protection from secondary exposure are equally important. Remedies should not depend entirely upon the victim repeatedly discovering every new URL or account. Technology-assisted matching can help identify substantially identical material, provided that such measures are governed by accuracy and procedural safeguards.

## CONSTITUTIONAL LIMITS: PRIVACY, DIGNITY AND FREEDOM OF EXPRESSION

Deepfake regulation cannot be separated from **Article 19(1)(a)**. Synthetic media can be harmful, but the fact that content is artificial does not by itself make it unlawful. Political satire, parody, artistic works, film production, educational demonstrations and research may all involve synthetic representations. A regulation that criminalises falsity without considering purpose, context and harm could extend beyond constitutionally permissible restrictions.<sup>18</sup>

---

<sup>16</sup> *Dr. Aniruddha Dhairyadhar Joshi v. John Does/Ashok Kumars & Ors.*, CS(COMM) 178/2026, Order (Delhi H.C. Feb. 24, 2026).

<sup>17</sup> *Raghav Chadha v. Ashok Kumar/John Doe & Ors.*, CS(OS) 466/2026, Order (Delhi H.C. July 1, 2026).

<sup>18</sup> INDIA CONST. art. 19(1)(a), (2)

*Shreya Singhal v. Union of India* provides an important constitutional lesson. The Supreme Court struck down section **66A** of the **Information Technology Act** because its broad and vague restrictions on online speech were incompatible with **Article 19(1)(a)**. The decision demonstrates that the existence of a technological harm does not eliminate the requirement of legal clarity and proportionality. Deepfake regulation should therefore define prohibited conduct with sufficient precision and provide procedural safeguards against arbitrary removal or punishment.<sup>19</sup>

**Article 21** strengthens the case for protection against malicious synthetic identity abuse. Privacy, dignity and personal autonomy may be seriously affected where a person's identity is appropriated without consent. The challenge is to design regulation that protects these interests without creating a general legal right to suppress criticism or unflattering representations. The distinction between unlawful impersonation and legitimate expression should remain central.

A proportionate regulatory model should therefore distinguish at least between: (a) synthetic content created for legitimate expressive purposes; (b) misleading content that creates significant but non-criminal harm; and (c) synthetic content used intentionally to commit or facilitate an established offence. Different categories can justify different interventions. Criminal punishment should be reserved for conduct satisfying criminal-law requirements, while labelling, correction and civil remedies can address lower-level harms.

## HYPOTHESIS

India's emerging synthetic-media regulatory framework represents a significant shift from reactive prosecution towards preventive platform governance; however, its effectiveness remains limited unless intermediary obligations are accompanied by clear allocation of responsibility, reliable provenance mechanisms, specialised digital-evidence procedures and accessible victim-centred remedies.

## POSSIBLE REFORMS

There is a need for a **comprehensive and technology-neutral legal framework** specifically addressing harmful deepfake content in India. The law should clearly define deepfakes and distinguish between legitimate uses, such as education, entertainment, satire and research, and

---

<sup>19</sup> *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, 80–89 (India).

unlawful uses involving fraud, impersonation, defamation, sexual exploitation, harassment or misinformation. The existing provisions of the **Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023 and IT Rules, 2021** should be strengthened and coordinated to provide clear criminal liability and effective civil remedies. **Mandatory labelling and digital provenance mechanisms** should be introduced for specified AI-generated or materially manipulated content so that users can identify synthetic media.

Intermediaries and AI platforms should be required to establish **quick and accessible reporting and takedown mechanisms**, particularly for non-consensual intimate deepfakes, impersonation and serious harassment, while also preserving relevant digital evidence for investigation. India should strengthen **cyber-forensic laboratories and AI-based detection capabilities** and provide specialised training to police officers, prosecutors and judges regarding deepfake identification and electronic evidence under the BSA, 2023. Stronger mechanisms for **international cooperation and cross-border investigation** should also be developed because deepfake offences may involve foreign platforms, servers and offenders. Special measures should be introduced for **victim protection**, including confidentiality, legal assistance, counselling and prevention of repeated uploading of the same harmful content. At the same time, regulation should contain adequate safeguards to protect **freedom of speech and expression under Article 19(1)(a)** and prevent legitimate satire, journalism, artistic expression and political commentary from being unnecessarily restricted. Public awareness and digital-literacy programmes should also be promoted to help citizens recognise and report manipulated content. These reforms would help India develop a balanced framework that protects privacy, dignity, reputation and security while allowing responsible development and use of Artificial Intelligence.

## RESEARCH GAP

The existing discussion has often concentrated on whether general Indian criminal laws are adequate for deepfakes or whether India requires a dedicated deepfake statute. The present study addresses a different gap: the need to evaluate the emerging synthetic-media regime as an ecosystem of responsibility. It examines the interaction between creator liability, intermediary duties, provenance, electronic evidence and victim remedies, particularly after the 2026 amendments relating to synthetically generated information.

## **OBJECTIVES OF THE STUDY**

- a. **To understand** the concept, nature and technological development of deepfake videos and synthetic media.
- b. **To examine** the different forms of cybercrime facilitated through deepfake technology, including identity theft, impersonation, fraud, defamation, cyberstalking, online harassment and non-consensual intimate imagery.
- c. **To analyse** the existing Indian legal framework applicable to deepfake-related offences, particularly the Information Technology Act, 2000, IT Rules, 2021 and Bharatiya Nyaya Sanhita, 2023.
- d. **To examine** the provisions of the Bharatiya Sakshya Adhiniyam, 2023 relating to electronic records and the challenges of establishing the authenticity and reliability of deepfake-related digital evidence.
- e. **To study** the constitutional issues concerning privacy, dignity, reputation and freedom of speech and expression in relation to deepfake content.
- f. **To analyse** the role and liability of social-media intermediaries and AI platforms in detecting, labelling and removing harmful deepfake content.
- g. **To examine** the judicial approaches adopted by Indian courts in cases involving AI-generated content, personality rights, privacy and unauthorised use of a person's identity.
- h. **To identify** the major legal, technological, evidentiary, investigative and jurisdictional challenges in controlling deepfake-related cybercrime.
- i. **To comparatively examine** selected international approaches to the regulation of deepfake and synthetic media.
- j. **To suggest** appropriate legal and regulatory reforms for preventing misuse of deepfake technology and strengthening victim protection in India.

## CONCLUSION

Deepfakes expose a structural weakness in conventional cybercrime regulation: digital content can be created cheaply, distributed instantly, copied repeatedly and contested after the harm has already occurred. The legal response therefore cannot depend exclusively upon identifying and prosecuting the original creator. India's regulatory landscape has moved beyond the earlier stage in which deepfakes were addressed only through general provisions of the IT Act and criminal law. The 2026 amendments to the IT Rules create a more specific governance framework for synthetically generated information and place greater responsibility upon intermediaries.<sup>20</sup>

Nevertheless, regulation should not be judged by the existence of labelling duties alone. The more difficult questions concern attribution, evidentiary authenticity, platform decisionmaking, victim access to remedies and constitutional limits. The accountability chain developed in this paper demonstrates that each stage of the synthetic-media lifecycle requires a different legal response. Criminal law addresses intentional unlawful conduct; intermediary regulation addresses dissemination; evidentiary law addresses authenticity; civil and personality-rights remedies provide immediate relief; and constitutional safeguards protect legitimate expression.

The hypothesis is therefore substantially supported: India's emerging framework is more developed than a simple “legal vacuum” description suggests, but its effectiveness depends upon coordination among legal rules, platforms, investigators, forensic institutions and courts. India does not necessarily require a technology-specific criminal prohibition covering every deepfake. It requires a coherent, rights-based system in which harmful synthetic media can be identified, attributed, removed and litigated without sacrificing legitimate uses of artificial intelligence.

The ultimate objective should be to protect human identity, dignity, privacy and public trust while preserving technological innovation and freedom of expression. Deepfake governance will remain a continuing regulatory task because the technology will evolve. A flexible accountability framework, supported by reliable evidence procedures and accessible victim

---

<sup>20</sup> Ministry of Electronics & Information Technology, Government of India, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026).

remedies, offers a more durable response than legislation focused narrowly on today's particular generation of synthetic-media tools.