

Research Article**BEYOND THE DEEFAKE: REASSESSING INDIA'S TECHNO-LEGAL
FRAMEWORK FOR SYNTHETIC MEDIA****Dr. Suman Surela**

Assistant Professor, Government Law College, Bundi.

Corresponding Author: Dr. Suman Surela.**Abstract**

The swift advancement of deepfake technology has altered the landscape of digital fraud, presenting intricate issues for privacy, dignity, reputation, personal autonomy, financial stability, and democratic dialogue. India has traditionally tackled the problems associated with deepfakes through disparate elements of cyber, criminal, data protection, and intermediary legislation. The introduction of a regulatory structure for synthetically produced information signifies a notable advance in the focused regulation of synthetic media. This article rigorously analyses India's developing techno-legal structure regarding deepfakes, focusing on intermediary accountability, transparency, detection methods, victim safeguarding, and constitutional protections. It additionally employs a comparative lens by analysing specific methodologies in the United States, European Union, China, and United Kingdom. The article contends that efficient regulation should go beyond merely eliminating content and imposing criminal penalties to include explicit legal criteria, trustworthy provenance systems, accessible victim recourse, and commensurate platform responsibility. It culminates by suggesting a rights-oriented and technologically flexible framework that can mitigate deepfake damages while safeguarding authentic expression and technology advancement.

Keywords: Deepfakes; Synthetic Media; Artificial Intelligence; Privacy; Digital Rights; Intermediary Liability; Platform Accountability; AI Regulation.

1. INTRODUCTION**1.1 Rise of Deepfakes and Synthetic Media**

Artificial intelligence has significantly altered the way digital material is produced, modified, and distributed. One of its most significant advancements is the advent of "deepfakes"—artificially created audio-visual or digitally altered material that can convincingly portray an individual as engaging in actions or uttering words that never took place. While synthetic media serves valid purposes in entertainment, education, accessibility, and creative expression, its growing availability has concurrently facilitated impersonation, fraud, harassment, misinformation, and non-consensual intimate photography. The original article delineates face-swapping, lip synchronisation, voice replication, and complete body reenactment as the primary methods of such manipulation.¹

1.2 Nature and Legal Harm

The legal challenges presented by deepfakes stem from their ability to impact multiple legally safeguarded interests at once. A solitary altered video can affect privacy, dignity, reputation, identification, intellectual property, financial stability, and protection from harassment. The issue

¹ Suruchi, *Deepfakes and the Law: A Comprehensive Comparative Analysis of Indian and International Legal Frameworks*, pp. 2–6.

intensifies notably when synthetic content is employed for non-consensual sexual depictions, political deceit, identity-related fraud, or damage to reputation. In contrast to traditional types of misinformation, deepfakes can exhibit a level of visual or auditory authenticity that hinders prompt validation and amplifies the rapidity and extent of distribution.

1.3 India's Regulatory Transition

India has traditionally tackled deepfake-related offences by utilising a blend of regulations from the Information Technology Act, 2000, the Information Technology Rules, 2021, criminal legislation, and data protection standards.² This disjointed strategy has offered potential solutions for specific damages but has not traditionally formed a thorough framework dedicated to deepfakes. The regulatory framework has significantly evolved with the introduction of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, which establish a specific structure for "synthetically generated information" and enhance intermediary responsibilities regarding prevention, labelling, metadata, and technical provenance.³

1.4 Research Problem and Scope

The primary issue is no longer merely the applicability of current rules to deepfakes, but rather if the new regulatory framework is adequately explicit, enforceable, and compatible with rights to tackle the unique harms posed by synthetic media. The article investigates this issue via India's legal and regulatory structure, constitutional tenets, intermediary obligations, issues related to evidence and enforcement, victim compensation, and certain comparable methodologies.

1.5 Central Argument of the Paper

This article contends that successful regulation of deepfakes necessitates approaches beyond mere criminalisation or the elimination of material. An integrated techno-legal framework necessitates the amalgamation of explicit legal norms, dependable identity and provenance systems, commensurate platform accountability, accessible remedies for victims, and robust enforcement. Simultaneously, regulation must align with constitutional safeguards of privacy, dignity, and freedom of expression. India's task is to govern detrimental synthetic media while not deeming technical innovation or synthetic expression as intrinsically illegal.

2. REVIEW OF LITERATURE

The existing literature on deepfakes has developed across technological, socio-legal and regulatory dimensions. However, much of the scholarship predates India's recent transition towards a specific **Synthetic Generated Information (SGI)** regulatory framework. The principal strands of literature relevant to the present study are as follows:

1. Rob Cover examines deepfakes as a developing form of audio-visual deception and emphasises their capacity to generate social anxiety concerning authenticity, trust and regulation. His work is useful for understanding why synthetic media should be examined not merely as technological innovation but as a challenge to established assumptions about digital truth and representation.⁴

2. Andrew Ray analyses the relationship between deepfakes, disinformation and democratic processes, arguing that existing legal mechanisms may be inadequate against technologically sophisticated forms of manipulated content. His analysis supports the need to reconsider legislative responses while accounting for the implications for democratic communication.⁵

² Information Technology Act, 2000, §§ 66C, 66D, 66E, 67, 67A, 69A & 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Ministry of Electronics and Information Technology, Government of India (10 Feb. 2026).

⁴ Rob Cover, "Deepfake Culture: The Emergence of Audio-Video Deception as an Object of Social Anxiety and Regulation," 36 *Journal of Media & Cultural Studies* 4 (2022).

⁵ Andrew Ray, "Disinformation, Deepfakes and Democracies: The Need for Legislative Reform," 44 *University of New South Wales Law Journal* 983 (2021).

3. The literature on Indian regulation generally approaches deepfakes through existing provisions of the Information Technology Act, 2000, intermediary regulation, criminal law and privacy principles. The source article similarly identifies the fragmented character of these remedies and highlights difficulties concerning attribution, enforcement, platform responsibility and victim protection.

4. Comparative scholarship increasingly examines disclosure, platform accountability and regulatory models adopted in the United States, European Union, China and the United Kingdom. These approaches demonstrate that regulation may focus not only on criminalisation but also on transparency, provenance, intermediary duties and risk management.

5. Emerging Indian commentary considers Bharatiya Nyaya Sanhita, 2023 and developing intermediary regulations as possible responses to synthetic-media harms. However, the literature remains comparatively underdeveloped concerning the constitutional limits, evidentiary consequences and practical operation of India's newer SGI framework.

Research Gap

The primary deficiency resides in the lack of a thoroughly integrated evaluation of India's 2026 SGI regulatory environment. Current scholarship often analyses deepfakes via traditional cyber-legal frameworks or through comparative regulatory approaches. The current research investigates if the developing Indian framework sufficiently balances privacy, dignity, expression, platform responsibility, origin, enforcement, and victim remedies, while safeguarding legitimate applications of synthetic media.

3. RESEARCH OBJECTIVES

The present study seeks to achieve the following objectives:

1. **To examine** the nature, characteristics and principal legal harms associated with deepfakes and synthetic media.
2. **To critically analyse** India's existing legal framework, including the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Digital Personal Data Protection framework and the 2026 SGI regulations.
3. **To assess** the constitutional implications of deepfake regulation concerning privacy, dignity and freedom of expression.
4. **To examine** platform accountability, detection, provenance, evidentiary reliability and victim remedies.
5. **To identify** regulatory gaps and develop legally sustainable, technology-neutral recommendations for India.

4. HYPOTHESIS

H₀ (Null Hypothesis): India's current and forthcoming legal structures, encompassing the 2026 SGI regulatory framework, are sufficient to tackle the primary legal issues stemming from deepfakes and synthetic media.

H₁ (Alternative Hypothesis): India's current and developing techno-legal structure, even with the enhancement of regulation via the 2026 SGI framework, is insufficient to thoroughly tackle the harms associated with deepfakes due to persistent deficiencies in constitutional protections, platform responsibility, detection and attribution, evidentiary dependability, cross-border enforcement, and victim-oriented remedies.

5. RESEARCH METHODOLOGY

The current research employs a doctrinal and comparative legal research approach. It fundamentally depends on primary legal materials, such as statutes, subordinate legislation, judicial rulings, and governmental regulatory documents, augmented by pertinent academic literature and credible secondary sources. The research rigorously analyses India's legal structure pertaining to deepfakes and synthetic media, focusing on the Information Technology Act of 2000, the Bharatiya Nyaya Sanhita of 2023, the Digital Personal Data Protection framework, the Information Technology Rules, and the 2026 SGI regulatory framework. A comparative examination of chosen jurisdictions is conducted to discern regulatory strategies related to transparency, platform responsibility, origin verification, enforcement, and victim safeguarding.

The study also assesses these frameworks in relation to constitutional tenets of privacy, dignity, and freedom of speech, aiming to pinpoint legal deficiencies and formulate a balanced, technology-agnostic regulatory strategy for India.

6. UNDERSTANDING DEEPFAKES AND THEIR LEGAL HARMS

6.1 Concept and Characteristics

Deepfakes represent a notable class of synthetic media generated or altered via artificial intelligence and machine-learning methodologies to fabricate authentic portrayals of individuals, occurrences, or assertions that may not align with reality. Their defining characteristic is not merely digital modification, but the growing capacity to render synthetic audio-visual content seemingly genuine. The foundational technologies comprise generative adversarial networks, facial interchange, lip synchronisation, and vocal replication.⁶

The legal challenge stems from the intersection of technical accuracy and ambiguous legitimacy. Traditional beliefs that images, audio recordings, or films serve as trustworthy proof of an occurrence are becoming increasingly challenging to uphold since synthetic media can convincingly imitate an individual's appearance, voice, or behaviour.⁷

6.2 Forms of Synthetic Media

Synthetic media includes several types, such as face-swapped movies, altered facial expressions, lip-synced recordings, replicated voices, complete body reenactments, and AI-generated dialogues or text. These methods can fulfill valid objectives in entertainment, education, accessibility, and artistic expression. Thus, the legal matter cannot be simplified to the simple presence of synthetic material; the pertinent inquiry is whether its generation or distribution results in legally recognisable damage.

6.3 Principal Legal Harms

Deepfakes can produce concurrent detriments related to privacy, dignity, reputation, identity, financial stability, and individual liberty. Significant dangers emerge from non-consensual personal visuals, impersonation, deception, extortion, social manipulation, and intentionally deceptive public messaging.⁸

These damages also generate unique challenges in evidence collection and enforcement. A victim could find it challenging to identify the originator or distributor of the content, and the swift proliferation across several platforms can render removal transient or insufficient. The transnational aspect of digital distribution exacerbates issues related to jurisdiction and enforcement.

Consequently, deepfakes necessitate a legal framework that is harm-oriented and contextually aware, differentiating between malevolent alterations and legitimate synthetic representation.

7. INDIA'S LEGAL FRAMEWORK: FROM FRAGMENTED REMEDIES TO SGI REGULATION

India lacks a singular, all-encompassing law governing deepfakes. Their legal ramifications are managed by an amalgamation of cyber law, criminal law, data protection rules, and intermediary regulation. The introduction of the Synthetic Generated Information (SGI) framework in 2026 signifies a crucial legislative shift as it explicitly includes technology-generated or altered information within intermediary due-diligence responsibilities.⁹

⁶ Rob Cover, "Deepfake Culture: The Emergence of Audio-Video Deception as an Object of Social Anxiety and Regulation," 36 *Journal of Media & Cultural Studies* 4 (2022).

⁷ Bobby Chesney & Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," 107 *California Law Review* 1753 (2019).

⁸ Andrew Ray, "Disinformation, Deepfakes and Democracies: The Need for Legislative Reform," 44 *University of New South Wales Law Journal* 983 (2021).

⁹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Ministry of Electronics and Information Technology, Government of India, 10 February 2026. The amendments introduce specific provisions concerning "synthetically generated information" and associated intermediary due diligence.

7.1 Information Technology Act, 2000

The Information Technology Act of 2000 serves as a crucial basis for tackling wrongdoing associated with deepfakes. Sections 66C and 66D may pertain to instances when synthetic content enables identity theft or impersonation, whilst Section 66E concerns breaches of privacy, and Sections 67 and 67A could be applicable to specific obscene or sexually explicit digital information. Section 79 offers a conditional intermediary safe harbour, contingent upon legislative stipulations and mandated due diligence.¹⁰ The challenge lies in the fact that these regulations were not explicitly formulated for AI-generated content, necessitating the adaptation of the underlying deepfake actions into established legal frameworks.

7.2 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 enhances the technology-specific framework by introducing crimes that can tackle behaviours linked to synthetic media. Specifically, the act of cheating by personation as outlined in Section 319 may be pertinent when a deepfake is employed to mimic another individual for fraudulent intentions.¹¹ Depending on the specific circumstances, additional regulations on cheating, forgery, criminal intimidation, defamation, or offences against women may also apply. The BNS offers a significant criminal law reaction; nonetheless, it does not establish a separate crime for the creation or distribution of a deepfake solely due to its synthetic nature.

7.3 Digital Personal Data Protection Framework

The Digital Personal Data Protection Act, 2023 introduces a distinct privacy-centric aspect. The objective is to govern the handling of digital personal information while acknowledging the individual's right to safeguard such data.¹² This framework could be applicable in situations when recognisable facial photos, vocal recordings, or other personal characteristics are handled within its legal parameters. Nonetheless, data protection legislation and deepfake regulation tackle disparate issues: the former primarily pertains to the handling of personal information, while the latter also include fraud, impersonation, reputational harm, and the distribution of counterfeit representations.

7.4 IT Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 created an extensive due-diligence framework for intermediaries. Regulation 3 mandates that intermediaries implement appropriate actions to combat certain types of illegal or detrimental information, encompassing data that violates privacy, misleads or deceives users, or is evidently untrue and misleading.¹³ The Rules thereby established an implicit regulatory foundation for addressing detrimental synthetic content prior to the implementation of a specific SGI framework.

7.5 2026 IT Amendment Rules

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 signify the most substantial regulatory advancement for synthetic media in India. The modifications establish particular responsibilities related to SGI, encompassing user awareness, the prevention of illegal SGI, and systems for labelling and technical origin. The framework furthermore tackles content that inaccurately depicts a natural individual, occurrence, or other topics by altering identify, voice, behaviour, actions, or assertions. Non-exempt SGI must adhere to significant labelling and technical identification/provenance mandates, whereas

¹⁰ Information Technology Act, 2000, §§ 66C, 66D, 66E, 67, 67A & 79.

¹¹ Bharatiya Nyaya Sanhita, 2023, § 319 (cheating by personation).

¹² Digital Personal Data Protection Act, 2023, Act No. 22 of 2023, Preamble.

¹³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(b).

intermediaries are obligated to avert the removal or modification of these labels and metadata as stipulated.¹⁴

The importance of the 2026 framework is in its transition from content-specific criminalisation to technology-aware intermediary regulation. However, its efficacy relies on the accuracy of its definitions, technical viability, enforcement capability, safeguarding of valid synthetic expression, and the provision of appropriate remedies for victims. The structure thus signifies a significant legislative advancement, however it may not constitute a comprehensive legal remedy for the deepfake issue.

8. CONSTITUTIONAL DIMENSIONS: PRIVACY, DIGNITY AND FREEDOM OF EXPRESSION

Assessment of deepfake regulation cannot be conducted exclusively from the perspective of technological oversight. Given that synthetic media can encompass an individual's likeness, vocalisation, identity, and expression, regulatory frameworks must function within the constitutional parameters of privacy, dignity, and freedom of speech and expression. The primary constitutional dilemma is to avert evident injury while avoiding excessive limitations on lawful expression.

8.1 Article 21 and Informational Privacy

The Supreme Court's acknowledgement of privacy as a constitutionally safeguarded right under Article 21 establishes a crucial basis for tackling the evils associated with deepfakes. Privacy entails personal sovereignty and governance over elements of one's identity and data. The illegal alteration and distribution of an individual's picture, voice, or other recognisable characteristics may consequently engage the informational and decisional aspects of privacy, especially when such content is personal, misleading, or exploitative.

8.2 Right to Dignity and Protection of Personal Identity

Deepfakes may undermine the constitutional principle of human dignity by attributing false actions or remarks to a recognisable person. The harm is most pronounced when artificial content portrays sexual activities, unlawful actions, or other humiliating behaviours that the person did not engage in. The safeguarding of individual identity and autonomy constitutes a significant constitutional factor in the governance of detrimental synthetic media.¹⁵

8.3 Article 19(1)(a) and Freedom of Expression

Synthetic media is not intrinsically illegal. Satire, satire, artistic creations, political discourse, education, and entertainment can appropriately utilise synthetic or altered material. Legislation that categorises all artificial or AI-generated representations as illegal may subsequently encumber Article 19(1)(a). The constitutional issue is not merely if the material is fabricated, but rather if the limitation targets a legally recognisable injury and is adequately linked to the acceptable bases for restriction.¹⁶

8.4 Reasonable Restrictions and Deepfake Regulation

Article 19(2) allows for justifiable limitations on the right to free speech and expression based on designated criteria. Consequently, limitations aimed at fraud, defamation, public order, incitement, or other constitutionally acknowledged objectives must fulfill the criteria of legality, necessity, and proportionality. The Supreme Court's legal principles on intermediary regulation warn against ambiguous or overly expansive limitations that could lead to the undue suppression of legitimate expression.¹⁷

¹⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Ministry of Electronics and Information Technology, Government of India, 10 February 2026.

¹⁵ *Id*

¹⁶ Constitution of India, arts. 19(1)(a) & 19(2).

¹⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

8.5 Satire, Parody, Artistic Expression and Legitimate Synthetic Media

A sustainable regulatory structure must consequently differentiate between detrimental deceit and authentic synthetic representation. Compulsory labelling, origin verification systems, and context-aware enforcement could offer a more lenient approach to tackling fraud compared to an outright ban. The aim must be to govern the detrimental application of synthetic media while safeguarding technological advancement, artistic expression, satire, and authentic public dialogue.

9. PLATFORM ACCOUNTABILITY, EVIDENCE AND VICTIM REMEDIES

The efficacy of deepfake regulation is largely contingent upon the actions of intermediaries, as platforms often govern the infrastructure utilised for the creation, uploading, replication, and distribution of synthetic content. The 2026 regulatory framework so transcends a passive middleman role by enforcing more stringent requirements regarding illegal SGI, technical protocols, labelling, and complaint resolution.¹⁸

9.1 Intermediary Responsibility

Intermediaries hold a pivotal role between artists, victims, and the broader public. The 2026 changes mandate suitable technical measures to avert the generation or distribution of illegal SGI and impose further responsibilities for user awareness and platform due diligence.¹⁹ This method enhances accountability, although an overdependence on automated moderation could lead to the erroneous elimination of content when it is unclear or context-sensitive.

9.2 Detection, Labelling and Provenance

Detection in isolation cannot yield a comprehensive resolution, as detection methods may become increasingly unreliable with the advancement of generative systems. The 2026 framework consequently embraces a supplementary strategy grounded in notable labelling and technological origin. Permissible SGI must adhere to the relevant framework by incorporating identifiable marking and enduring information or other suitable technological provenance methods where technically practicable.²⁰ Provenance can aid users, investigators, and judicial bodies in evaluating the source and subsequent management of synthetic material, albeit its efficacy relies on technical compatibility and resilience against tampering.

9.3 Attribution and Cross-Border Enforcement

A primary challenge persists in determining the individual who initially created or distributed a deepfake. Content can be generated without attribution, disseminated across many legal territories, and replicated by numerous individuals. As a result, measures for identification at the platform level and collaboration with law enforcement agencies are crucial for effective attribution.²¹ Cross-border enforcement, meanwhile, persists in presenting jurisdictional and evidential challenges that cannot be addressed exclusively through local intermediary responsibilities.

¹⁸ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Ministry of Electronics and Information Technology, Government of India, 10 February 2026.

¹⁹ Id.; see also Ministry of Electronics & Information Technology, Government of India, *Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes*, Press Information Bureau, 6 August 2026.

²⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), r. 3(3), concerning prominent labelling and permanent metadata or other appropriate technical provenance mechanisms.

²¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2), concerning identification of the first originator in specified circumstances; see also Ministry of Electronics & Information Technology, Government of India, *Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes*, 6 August 2026.

9.4 Admissibility and Reliability of Synthetic Evidence

The growing accessibility of AI-produced content also influences the evidential significance of digital recordings. Judicial bodies might have to examine the origin, authenticity, metadata, chain of custody, and production techniques of digital evidence instead of presuming that audio-visual material is genuine only based on its realistic appearance. The advent of synthetic evidence thus underscores the necessity for proficient forensic analysis.

9.5 Victim-Centred Remedies

Protection for victims should encompass more than just the elimination of the harmful content. The 2026 framework enhances complaint procedures and offers swift resolutions for issues such as impersonation and specific intimate or sexually explicit content. Efficient safeguarding must also promote the conservation of evidence, rehabilitation of reputation, identification of culpable parties, and suitable recompense when legally permissible. A victim-focused framework is essential to guarantee that deepfake legislation tackles not just the presence of illegal material but also the ongoing repercussions of its distribution.

10. COMPARATIVE PERSPECTIVES: LESSONS FOR INDIA

Empirical evidence indicates that several jurisdictions have implemented diverse regulatory approaches to tackle deepfakes, encompassing transparency and provenance requirements, platform responsibilities, and specific criminal crimes. The significance of these models for India is not in their complete adoption, but in recognising regulatory mechanisms that can enhance the developing Synthetic Generated Information (SGI) environment.

10.1 United States

The United States has adopted a relatively disjointed strategy, integrating federal programs with state legislation and pre-existing civil and criminal remedies. A notable recent advancement is the TAKE IT DOWN Act, which tackles the intentional dissemination of non-consensual intimate visual representations, encompassing digitally altered materials, and sets forth responsibilities regarding the elimination of such material.²² This method demonstrates the significance of legislation tailored to specific harms, especially for non-consensual intimate deepfakes. The disjointed character of regulation across many legal frameworks and jurisdictions illustrates the challenges in establishing consistent standards for synthetic media.

10.2 European Union

The European Union has embraced a more cohesive transparency-focused strategy via the Artificial Intelligence Act. Article 50 mandates that creators of systems producing synthetic music, images, videos, or text content must label their outputs in a machine-readable manner that may be identified as artificially generated or altered.²³ Deployers must also disclose deepfake content in circumstances covered by the Act.²⁴

Significantly, the EU framework acknowledges that not all synthetic representations have identical regulatory risks. The regulations on transparency so differentiate deepfakes from specific artistic, creative, satirical, and fictional creations, where disclosure should be executed in a way that does not unduly disrupt the work.²⁵ For India, this offers a valuable regulatory guideline:

²² *Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act*, S. 146, 119th Cong. (2025) (TAKE IT DOWN Act). The legislation addressed non-consensual intimate visual depictions, including digitally manipulated depictions, and platform removal obligations.

²³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), art. 50(2).

²⁴ European Commission, *Transparency Obligations under Article 50 of the AI Act*, explaining the obligations applicable to providers and deployers concerning AI-generated or manipulated content and deepfakes.

²⁵ European Commission, *Guidelines on the Implementation of the Transparency Obligations for Certain AI Systems under Article 50 of the AI Act* (20 July 2026); see also European Commission, *Code*

transparency may occasionally be more advantageous than outright prohibition, especially where synthetic content is not intrinsically detrimental.

10.3 China

China has implemented a very straightforward regulatory framework via its Provisions on the Administration of Deep Synthesis of Internet-based Information Services, effective from 10 January 2023.²⁶ The framework pertains to technologies that can create or significantly modify information, such as synthetic voices, face production, face replacement, facial manipulation, and posture alteration.

The Chinese system prioritises notable identification and technological traceability. Providers of designated deep-synthesis services must prominently identify generated or modified content, whereas organisations and people are forbidden from technically eliminating, modifying, or obscuring mandated deep-synthesis markers. The Indian 2026 SGI framework likewise integrates labelling and provenance systems. The relative importance thus resides in acknowledging that technical provenance must function as an integral element of platform governance instead of simply being an ancillary attribute.

10.4 United Kingdom

The United Kingdom has systematically advanced certain safeguards against synthetic intimate pictures. The Online Safety Act 2023 rendered the deliberate dissemination or intimidation over the distribution of intimate images or videos without consent illegal under certain conditions.²⁷ The Data (Use and Access) Act 2025 subsequently established offences related to the production or solicitation of the production of alleged intimate photos of adults without consent or a reasonable belief in consent.²⁸ The statute also acknowledges that a "supposed intimate image" could be an image that seems to portray an individual but is not, or is not solely, a genuine photograph or video of that person.²⁹

The UK's strategy illustrates the importance of overseeing both the distribution and the production and commissioning of especially detrimental types of synthetic content. This prompts India to consider whether particular types of deepfake harm, namely non-consensual intimate images, necessitate distinct substantive offences instead of solely depending on standard cybercrime laws.

10.5 Selected Asia-Pacific Approaches

The extensive Asia-Pacific context demonstrates significant diversity in regulatory frameworks. Certain nations have depended on specific criminal regulations, but others have prioritised platform responsibility, transparency, and content recognition. These methods illustrate that no singular legislative framework offers a comprehensive solution to the intricate technological and legal challenges posed by synthetic media.

The comparison data, however, uncovers multiple consistent regulatory tenets: explicit definitions, origin tracking systems, platform responsibility, swift victim redress, dependable identification, and safeguarding of legitimate expression. India's 2026 SGI framework integrates

of Practice on Transparency of AI-Generated Content (2026). The Commission explains that artistic, creative, satirical and fictional works receive context-sensitive treatment under the transparency regime.

²⁶ *Provisions on the Administration of Deep Synthesis of Internet-based Information Services*, Cyberspace Administration of China, effective 10 January 2023.

²⁷ Online Safety Act 2023, c. 50, §§ 188–189 (U.K.), inserting §§ 66B–66C into the Sexual Offences Act 2003.

²⁸ Data (Use and Access) Act 2025, c. 18, § 138 (U.K.), inserting provisions into the Sexual Offences Act 2003 concerning the creation or requesting of purported intimate images without consent.

²⁹ Data (Use and Access) Act 2025, c. 18, explanatory notes, paras. 1009–1018, explaining the statutory meaning of "purported intimate image" and the offences concerning its creation or commissioning.

numerous of these components, especially via intermediate due diligence, marking, and technological provenance. The primary objective of Indian law is to establish these systems with adequate clarity, technical viability, and constitutional balance, rather than merely replicating the regulatory framework of another nation.

11. CRITICAL ANALYSIS: REGULATORY GAPS AND THE WAY FORWARD

India's shift toward regulations related to SGI marks a notable advancement; nonetheless, the mere presence of legislative requirements does not inherently create an effective deepfake framework. The primary inquiry is whether the framework can convert technology need into explicit, enforceable, and constitutionally balanced legal safeguards. The source material highlights ongoing issues regarding definition, intermediary accountability, attribution, forensic capabilities, victim restitution, and freedom of expression.

11.1 Definition and Conceptual Clarity

A primary obstacle is preserving a clear understanding of what defines detrimental synthetic media. Previous Indian laws did not explicitly establish a thorough deepfake crime, necessitating that officials utilise existing statutes against impersonation, privacy, obscenity, fraud, or similar offences. The 2026 SGI framework enhances this stance by explicitly governing particular types of synthetic information; nonetheless, successful enforcement will still rely on clear differentiations between standard editing, authentic synthetic content, and significantly misleading or detrimental alterations.³⁰

11.2 Intermediary Regulation

The legal obligations imposed on intermediaries should align with their genuine technological capabilities and functions. Enhanced due-diligence requirements can enable swift action, although an overdependence on automated systems might lead to the removal of valid content just owing to its synthetic nature or challenges in verification. The objective is therefore to create platform responsibilities that are attuned to risk rather than engaging in arbitrary content censorship.

11.3 Detection and Attribution

The detection of deepfakes is fundamentally dynamic due to the concurrent evolution of generative technologies and detection methodologies. Attribution is further hampered by anonymity, encryption, the existence of many accounts, and transnational distribution. The original study likewise highlights the constraints of forensic expertise and the challenges in determining if content is generated by AI and produced with malicious intent. India necessitates enhanced investment in digital forensics, the safeguarding of metadata, and the development of institutional technological proficiency.

11.4 Victim Remedies and Compensation

Eliminating detrimental content constitutes merely one aspect of efficient remediation. Individuals affected by deepfakes may persist in experiencing reputational, psychological, occupational, and financial repercussions even subsequent to the removal of the initial content. A victim-focused framework need to enable swift expulsion, preservation of evidence, identification of culpable parties, and access to suitable civil or criminal recourse. The current system would improve with enhanced collaboration among intermediary complaint systems, law enforcement bodies, and judicial solutions.

11.5 Chilling Effects and Over-Removal

Regulation should also consider the potential for excessive extraction. Synthetic media can be appropriately utilised for parody, satire, artistic expression, educational purposes, and commentary. Considering technological manipulation as the harm could lead to a confusion

³⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Ministry of Electronics and Information Technology, Government of India, 10 February 2026; see also *supra* notes 16 & 28.

between form and illegality. Regulatory initiatives ought to concentrate on fraud, lack of permission, and evident damage while safeguarding constitutionally guarantyd expression.³¹

11.6 Cross-Border Enforcement

The distribution of deepfakes often surpasses geographical limits. A creator might function inside one legal framework, disseminate information via another, and aim at individuals in India. Legislation at the national level is insufficient to address such circumstances. India consequently requires enhanced global collaboration on the safeguarding of electronic evidence, the identification of offenders, cooperation among platforms, and transnational enforcement.

11.7 Adaptive and Technology-Neutral Regulation

Ultimately, the regulation of deepfakes ought to be technology-agnostic and flexible. A framework centred on a specific generation method may become outdated when novel types of synthetic media arise. India's regulatory framework ought to emphasise the attributes and detriments of synthetic content instead than imposing regulations solely on specific tools or algorithms. The aim should be a structure that can adapt to technology advancements while ensuring transparency, accountability, and constitutional protections.

12. FINDINGS AND SUGGESTIONS

The study indicates that India has transitioned from a mostly disjointed, offense-oriented strategy to a more technology-aware regulatory paradigm via the 2026 SGI framework. Nonetheless, regulatory acknowledgement does not inherently result in adequate safeguarding. Numerous significant and organisational deficiencies persist regarding conceptual precision, accountability, investigative capability, platform adherence, victim restitution, and constitutional protections.

The study makes the following suggestions:

1. **Develop clear statutory terminology:** Indian law should maintain precise distinctions between synthetic media, manipulated content and harmful/deceptive SGI, thereby reducing uncertainty in enforcement.
2. **Strengthen provenance infrastructure:** Labelling and metadata requirements should be supported by interoperable technical standards so that synthetic content can be identified across platforms.
3. **Adopt risk-based intermediary duties:** Platform obligations should correspond to the nature and severity of the harm, with safeguards against automated over-removal of lawful content.
4. **Establish specialised forensic capacity:** Cybercrime agencies and courts require trained personnel and reliable forensic mechanisms for examining authenticity, provenance and manipulation.
5. **Strengthen victim-centred remedies:** Victims should have accessible mechanisms for expedited removal, evidence preservation, identification of perpetrators and appropriate compensation or other relief.
6. **Improve cross-border cooperation:** International mechanisms for evidence preservation, attribution and enforcement should be strengthened to address jurisdictional difficulties arising from global dissemination.
7. **Protect legitimate expression:** Regulation should distinguish malicious deception from satire, parody, artistic, educational and other constitutionally protected synthetic expression.

The resulting framework should therefore combine **technological accountability with constitutional proportionality**, rather than treating prohibition as the default response.

³¹ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

13. CONCLUSION

The rise of deepfakes has shown a critical shortcoming in traditional digital regulatory methods: the law is increasingly faced with content whose perceived authenticity cannot be taken for granted. Synthetic media can promote authentic creativity and innovation; yet, its nefarious application may concurrently jeopardise privacy, dignity, reputation, identity, financial stability, and public confidence.

India's legal approach has thus transitioned from dependence on disparate elements of cyber and criminal legislation to a more technology-adaptive structure with the 2026 SGI revisions. The establishment of requirements related to synthetic data, labelling, origin, and intermediary due diligence signifies a significant regulatory advancement. Nonetheless, substantial enquiries persist concerning conceptual precision, technical implementation, attribution, forensic dependability, transnational jurisdiction, and adequate victim redress.

The comparative examination reveals that various jurisdictions have implemented diverse mixes of harm-specific criminalisation, transparency, provenance, platform responsibility, and victim protection. No individual approach, meanwhile, offers a comprehensive resolution. India's regulatory approach must consequently align with its constitutional principles, especially concerning the safeguarding of privacy, dignity, and freedom of expression.

Ultimately, proficient governance of deepfakes should aim not to eradicate synthetic media but to oversee detrimental applications of such media via explicit, balanced, and technology-agnostic criteria. A sustainable Indian framework should integrate preventive platform responsibilities with trustworthy provenance systems, expert forensic capabilities, accessible victim reparations, and protections against undue material deletion. This methodology can mitigate the genuine detriments posed by deepfakes while safeguarding the innovative, pedagogical, and technological potentials of synthetic media. The future of deepfake regulation in India should be perceived not as a dichotomy between innovation and regulation, but as an initiative to establish a legal framework that allows technological advancement to coexist with accountability, personal autonomy, and constitutional rights.

Citation: Dr. Suman Surela. 2026. "BEYOND THE DEEPFAKE: REASSESSING INDIA'S TECHNO-LEGAL FRAMEWORK FOR SYNTHETIC MEDIA". *International Journal of Academic Research*, 13(3): 237-258.

Copyright: ©2026 Dr. Suman Surela. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.