

Synthetic Media and Its Misuse in India: A Critical Legal Analysis of The Regulatory Framework, Judicial Response, and The Path Forward

Dr. Vikalp and Dr. Rituraj Sinha

Christ University

DOI: <https://doi.org/10.51244/IJRSI.2026.1307000027>

Received: 04 July 2026; Accepted: 09 July 2026; Published: 23 July 2026

ABSTRACT

The proliferation of synthetic media—commonly referred to as "deepfakes"—represents one of the most consequential technological disruptions of the twenty-first century, with India emerging as both a major producer and victim of AI-generated deceptive content. This article presents the first comprehensive legal analysis of India's regulatory response to synthetic media misuse, examining the recently notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, alongside the existing statutory framework under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and allied legislation. Drawing upon empirical data from government reports, market research, and judicial precedents, this study evaluates the adequacy of India's legal architecture in addressing the multifaceted harms of deepfakes, including non-consensual intimate imagery, electoral manipulation, financial fraud, and reputational damage. The article argues that while the IT Rules 2026 represent a watershed moment in Indian digital governance—featuring the world's most aggressive takedown timeline of three hours and mandatory 10% visual labelling requirements—significant gaps persist in enforcement capacity, cross-border jurisdiction, and the protection of ordinary citizens who lack the resources of celebrity litigants. Through comparative analysis with the European Union's AI Act, China's deepfake provisions, and Singapore's POFMA framework, this article proposes a multi-pronged reform agenda encompassing a dedicated Synthetic Media Act, enhanced judicial training, public-private detection partnerships, and constitutional safeguards for free expression.

Keywords: Synthetic Media, Deepfakes, Information Technology Act, 2000, IT Rules 2026, Bharatiya Nyaya Sanhita, 2023, Non-Consensual Intimate Imagery, Digital Governance, AI Regulation, Platform Accountability.

INTRODUCTION: THE SYNTHETIC MEDIA REVOLUTION AND ITS DARK UNDERBELLY

The Technology and Its Promise

Synthetic media refers to audio, visual, or audio-visual content that is artificially or algorithmically created, generated, modified, or altered using computational resources in a manner that appears authentic or true.¹ The underlying technologies—primarily Generative Adversarial Networks (GANs), autoencoders, diffusion models, and transformer architectures—have democratized content creation to an unprecedented degree. What once required Hollywood-level budgets and technical expertise can now be accomplished by anyone with a smartphone and access to freely available applications.²

The global deepfake AI market was valued at approximately USD 764.8 million in 2024 and is projected to reach USD 19.82 billion by 2033, growing at a compound annual growth rate (CAGR) of 44.3%.³ The Asia-Pacific region dominates this market with a 37.6% share, with India's market alone projected to reach USD 710 million by 2026.⁴ These figures underscore not merely a technological trend but a fundamental restructuring of how information is produced, consumed, and trusted in the digital age.

Table 1: Global Deepfake AI Market Projections (2024–2033)

Year	Market Size (USD Million)	Growth Rate (YoY)
2024	764.8	Base Year
2025	1,052.2	37.6%
2026	1,518.0	44.3%
2028	3,316.0	44.3% (CAGR)
2030	6,905.0	44.3% (CAGR)
2033	19,824.7	44.3% (CAGR)

Source: Grand View Research, Deepfake AI Market Report, 2025.

The legitimate applications of synthetic media are manifold and transformative. In healthcare, synthetic data enables medical research without compromising patient privacy. In education, AI-generated tutors can provide personalized instruction in vernacular languages. In entertainment, filmmakers use deepfake technology for digital de-aging and visual effects—over 45 major film productions employed such techniques in 2023 alone. In accessibility, text-to-speech and voice cloning technologies empower persons with disabilities.

The Misuse Epidemic

However, the same technologies that enable creative expression and social good have been weaponized with alarming speed and sophistication. The World Economic Forum's Global Risks Report 2024 identified AI-generated synthetic media as one of the top ten near-term global risks. ⁵Deepfake fraud surged over ten-fold globally from 2022 to 2023, with the cryptocurrency sector accounting for 88% of cases and fintech comprising 8%. ⁶

In India, the crisis is particularly acute. A 2023 McAfee survey revealed that 47% of Indian respondents had either been directly victimized by an AI voice scam or knew someone who had been—a figure significantly higher than the global average. ⁷Industry reports documented a 550% increase in detected deepfake content in India between 2019 and 2024. ⁸The confluence of India's massive digital user base—over 950 million internet users—rapidly improving AI accessibility, and relatively low digital literacy rates in rural areas has created what this article terms a "perfect storm" for synthetic media misuse. ⁹

The harms manifest across multiple domains:

1. **Non-Consensual Intimate Imagery (NCII):** Perhaps the most pervasive and psychologically devastating misuse involves the creation and distribution of sexually explicit deepfake content featuring individuals without their consent. Women, particularly public figures, bear a disproportionate burden. The November 2023 incident involving a 14-second face-swap deepfake of a leading Indian film actress—subsequently identified as Rashmika Mandanna—went viral across WhatsApp, X, and Telegram within hours, triggering nationwide outrage and catalyzing regulatory action.
2. **Electoral Manipulation:** During India's 2024 general elections, over 50 million AI-generated voice clone calls were deployed, with cheapfakes and deepfakes circulating at scale across regional languages. The Election Commission issued advisories urging political parties to abstain from synthetic media misuse, but enforcement proved challenging.

3. Financial Fraud: AI voice cloning has been weaponized for sophisticated financial scams, with fraudsters impersonating family members, business executives, and government officials to extract money from victims.
4. Reputational Harm and Defamation: Synthetic media enables the fabrication of statements, actions, and events attributed to real individuals, causing irreparable reputational damage that often outpaces legal remedies.
5. Document Forgery: AI-generated forged government identity documents, appointment letters, and official records present emerging threats to institutional integrity.

The Evolution of India's Legal Framework: From The It Act, 2000 to The it Rules, 2026

The Foundational Statute: Information Technology Act, 2000

India's primary legislation governing cyber activities, the Information Technology Act, 2000 (IT Act), was enacted in an era when synthetic media was the stuff of science fiction.¹⁰ Nevertheless, several provisions have been invoked—often creatively—to address deepfake-related offences.

Section 66C penalizes identity theft, prescribing imprisonment up to three years and a fine up to ₹1 lakh for fraudulent or dishonest use of any person's electronic signature, password, or other unique identification feature. In the Rashmika Mandanna case, the FIR was filed under this provision alongside Section 66E (privacy violation).

Section 66D addresses cheating by personation using computer resources, carrying imprisonment up to three years and a fine up to ₹1 lakh. This provision has proven particularly relevant for voice clone scams where perpetrators impersonate known individuals.

Section 66E protects against violations of privacy, including capturing, publishing, or transmitting images of a private area of any person without consent. While drafted with physical photography in mind, courts have interpreted its application to digitally manipulated intimate imagery.

Section 67 penalizes the publication or transmission of obscene material in electronic form, carrying imprisonment up to five years and a fine up to ₹10 lakh for a first conviction, and up to seven years for subsequent convictions.

Section 67A specifically addresses sexually explicit material, with enhanced penalties.

Section 69A empowers the Central Government to block public access to information through a structured executive process involving a designated committee, where such content threatens sovereignty, integrity, public order, or foreign relations.

Section 79 provides the critical "safe harbour" framework, exempting intermediaries from liability for third-party content provided they exercise "due diligence" and comply with government directions. This provision, read down by the Supreme Court in ¹¹Shreya Singhal v. Union of India, (2015) 5 SCC 1, ¹²requires "actual knowledge" through court order or government notification—not private complaint—to trigger loss of safe harbour protection.

The Bharatiya Nyaya Sanhita, 2023: The New Penal Code

The Bharatiya Nyaya Sanhita, 2023 (BNS), which superseded the Indian Penal Code, 1860, contains several provisions relevant to synthetic media misuse:

Section 336 of the Bharatiya Nyaya Sanhita, 2023 (Chapter XVIII) addresses forgery (making a false document) and its sub-clauses deal with forgery for various purposes, including forgery for cheating and forgery intended to harm reputation; AI-generated forged documents and fabricated electronic records would be prosecuted under these forgery provisions where the elements are satisfied.

Sections 318 and 319 of the Bharatiya Nyaya Sanhita, 2023 criminalize cheating and cheating by personation respectively, and are directly implicated in voice-clone scams and impersonation-based frauds that use computer resources to deceive victims.

Section 74 of the Bharatiya Nyaya Sanhita, 2023 (formerly IPC 354) penalizes assault or use of criminal force to a woman with intent to outrage her modesty, with punishment of imprisonment for a term not less than one year and which may extend to five years, and a fine; the provision's language and protective purpose mean that creation and distribution of non-consensual intimate deepfakes can, in appropriate cases, be framed as a digital form of this offence when the statutory elements are met.

Section 78 of the Bharatiya Nyaya Sanhita, 2023 (BNS) deals with stalking, including repeated monitoring, following, or contacting a woman, and its scope expressly contemplates electronic surveillance and misuse of online communication channels; therefore, persistent online monitoring, unwanted targeted distribution of synthetic media, or using digital means to harass a woman can attract liability under this provision.

Special Legislation

The Protection of Children from Sexual Offences Act, 2012 (POCSO): Section 14 penalizes the use of a child for pornographic purposes, carrying imprisonment of five to seven years and a fine. The creation of child sexual exploitative and abuse material (CSEAM) using deepfake technology attracts the most severe penalties under Indian law.

The Indecent Representation of Women (Prohibition) Act, 1986 (IRWA): Section 3 prohibits indecent representation of women through advertisements, publications, writings, paintings, figures, or in any other manner. Violations attract imprisonment up to two years and a fine up to ₹2,000 for first conviction, with enhanced penalties for subsequent offences.

The Representation of the People Act, 1951: While not specifically addressing synthetic media, provisions against false statements in relation to election candidates and corrupt practices could potentially be applied to deepfake electoral manipulation.

The IT Rules, 2021: The Regulatory Foundation

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under Section 87 of the IT Act, established a three-tier grievance redressal mechanism for digital media and imposed due diligence obligations on intermediaries. Key provisions included:¹³

Rule 3(1)(b): Requiring intermediaries to inform users not to host content that is defamatory, obscene, pornographic, pedophilic, or invasive of another's privacy.

Rule 3(1)(d): Mandating removal or disabling access to unlawful content within 36 hours of receiving court orders or government notifications.

Rule 4: Enhanced obligations for Significant Social Media Intermediaries (SSMIs) with over 5 million Indian users, including appointing Chief Compliance Officers, Nodal Contact Persons, and Resident Grievance Officers.

The IT Rules, 2026: India's Watershed Response

On February 10, 2026, the Ministry of Electronics and Information Technology (MeitY) notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (G.S.R. 120(E)), which came into force on February 20, 2026. These amendments represent India's first explicit statutory framework addressing synthetically generated information and constitute one of the most aggressive regulatory responses globally.¹⁴

Definition of Synthetically Generated Information (SGI)

Rule 2(1)(wa) defines 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.'¹⁵ The definition is deliberately technology-neutral and broad, encompassing deepfakes, voice clones, AI-generated images, and algorithmically manipulated media. Three critical exclusions are carved out:¹⁶

1. Routine editing activities (formatting, colour adjustment, noise reduction, transcription, compression) that do not materially alter substance, context, or meaning;
2. Routine creation of documents, presentations, and educational materials using illustrative or template-based content, provided no false document is created;
3. Use of computer resources solely to improve accessibility, clarity, quality, translation, or searchability without manipulating underlying content.

Prohibited and Permitted SGI

Rule 3(3) establishes a dual framework:

Prohibited SGI (must be prevented using automated tools): Child sexual exploitative and abuse material (CSEAM), non-consensual intimate imagery (NCII), and obscene or sexually explicit content; content creating false documents or false electronic records; content relating to explosives, arms, or ammunition; content falsely depicting individuals or events in a manner likely to deceive.

Permitted SGI (must be prominently labelled with visible markers for visual content and audio disclosures for audio content, plus embedded permanent metadata and unique identifiers).

The World's Most Aggressive Takedown Timeline

The amendments drastically compress compliance timelines:

Table 2: Takedown Timeline Comparison—India vs. Global Jurisdictions

Jurisdiction	Regulatory Framework	Takedown Timeline	Emergency Removal
India	IT Rules, 2026	3 hours	2 hours (NCII)
European Union	Digital Services Act, 2022	24 hours	Varies by Member State
United States	No Federal Standard	48+ hours	No federal mandate
Singapore	POFMA	24 hours	Case-by-case
United Kingdom	Online Safety Bill	24 hours	Case-by-case

Sources: MeitY Notification G.S.R. 120(E), 2026; EU Digital Services Act; Sumsub Global Deepfake Fraud Report.

The 3-hour takedown window for court orders and government notifications (reduced from 36 hours) and the 2-hour emergency removal for NCII content (reduced from 24 hours) make India's framework the most time-compressed globally. For user grievances, general complaints must now be resolved within 7 days (reduced from 15 days), identity theft complaints within 36 hours (reduced from 72 hours), and NCII complaints within 2 hours.

Enhanced SSMI Obligations

Rule 4(1A) imposes unprecedented pre-publication duties on Significant Social Media Intermediaries:

1. User Declaration: Requiring users to declare whether content is SGI before publication;
2. Technical Verification: Deploying automated tools to verify such declarations;
3. Prominent Labelling: Ensuring verified SGI is clearly labelled with appropriate notices.

The proviso to Rule 4(1A) clarifies that SSIMs knowingly permitting, promoting, or failing to act upon SGI in contravention of the Rules shall be deemed to have failed to exercise due diligence—thereby losing safe harbour protection under Section 79(1) of the IT Act.

The 10% Labelling Requirement

Rule 3(3)(a)(ii) mandates that SGI labels must cover at least 10% of the visual surface area or be audible for at least 10% of the audio duration. The label must be 'prominent' and cannot be removed, suppressed, or altered by the user. Additionally, SGI tools must embed a permanent unique metadata identifier at the point of generation—practically converging on the C2PA (Coalition for Content Provenance and Authenticity) framework.

User Awareness and Periodic Notices

Amended Rule 3(1)(c) requires intermediaries to inform users at least once every three months (increased from annually) about consequences of non-compliance, including potential criminal liability. For SGI-enabling intermediaries, additional warnings under Rule 3(1)(ca) must specify penalties under the Representation of the People Act, 1951, IRWA, 1986, Sexual Harassment at Workplace Act, 2013, and Immoral Traffic Act, 1956.

Judicial Response and Personality Rights Jurisprudence

The Emergence of Personality Rights in India

While statutory law has struggled to keep pace with synthetic media technology, Indian courts have developed a robust jurisprudence of personality rights that provides significant—though incomplete—protection against deepfake misuse. The Supreme Court in ¹⁷*R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632, ¹⁸recognized the right to privacy as implicit in Article 21 of the Constitution, including the right to be left alone. In Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¹⁹the Supreme Court unanimously affirmed privacy as a fundamental right, observing that 'the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21.'

The Delhi High Court has been particularly active in developing personality rights jurisprudence. In *Amitabh Bachchan v. Rajat Nagi*, CS (COMM) 493/2022, the Court granted an omnibus injunction protecting the actor's name, image, voice, and personality traits from unauthorized commercial use, observing that 'the celebrity's right of publicity is an enforceable right.'²⁰

The Deepfake Injunction Wave (2023–2025)

Between 2023 and 2025, the Delhi High Court issued a sustained string of personality-rights injunctions specifically addressing synthetic media threats:

Table 3: Notable Personality Rights Injunctions in India (2023–2025)

Case	Plaintiff	Relief Granted	Date
Amitabh Bachchan v. Rajat Nagi	Amitabh Bachchan	Omnibus injunction protecting name, image, voice, personality	2022
Anil Kapoor v. Simply Life India	Anil Kapoor	Injunction against unauthorized use of image, voice, likeness	2023
Jackie Shroff v. The Peppy Store	Jackie Shroff	Protection of personality rights including image and voice	2024
Singer v. AI Platform	Leading playback singer	Injunction against unauthorized voice cloning	2024
Journalist v. Social Media Platform	Senior journalist	Image protection injunction	2024
Yoga Guru v. AI App	Prominent yoga guru	Face and likeness protection	October 2025

Sources: Delhi High Court Orders; Vaish Law Associates Analysis.

Each of these cases followed a similar pattern: the plaintiff hired counsel, drafted a plaint, sat through hearings, and awaited an injunction order to be served on platforms. While these orders provided meaningful relief to named individuals, they were inherently narrower than legislation could be. The structural problem—the absence of a comprehensive framework protecting ordinary citizens—remained unaddressed.²¹

The Limitations of Judicial Remedies

The personality rights approach suffers from several critical limitations:

1. **Resource Asymmetry:** Celebrity litigants can afford specialized counsel and endure protracted litigation. Ordinary citizens—particularly women in rural areas who are disproportionately victimized by NCII deepfakes—lack comparable resources.
2. **Reactive Nature:** Injunctions are granted after harm has occurred. The viral nature of synthetic media means that by the time judicial relief is obtained, content has been replicated across multiple platforms and jurisdictions.
3. **Platform Fragmentation:** An injunction against one platform does not prevent dissemination across WhatsApp, Telegram, and encrypted channels where content moderation is technically challenging.
4. **Cross-Border Enforcement:** Many deepfake applications and hosting services operate from jurisdictions outside India, making enforcement of domestic court orders difficult.

Empirical Analysis: The Scale and Scope of Synthetic Media Misuse in India

Market Data and Growth Projections

Table 4: India Deepfake Technology Market Projections (2024–2030)

Year	Market Size (USD Million)	YoY Growth
2024	450	Base
2025	550	22.2%
2026	710	29.1%
2027	890	25.4%
2028	1,120	25.8%
2029	1,410	25.9%
2030	1,780	26.2%

Source: Fortune Business Insights, Deepfake Technology Market Report, 2025.

The India deepfake technology market is projected to nearly quadruple between 2024 and 2030, reflecting both legitimate commercial applications and the expanding misuse ecosystem.

The Detection Gap

The global deepfake detection software market was valued at USD 114.3 million in 2024 and is projected to reach USD 5,609.3 million by 2034, growing at a CAGR of 47.6%. However, detection technology consistently lags behind generation capabilities—a phenomenon this article terms the 'detection gap.'²²

Table 5: Detection Accuracy vs. Deepfake Sophistication (2019–2025)

Year	Detection Accuracy (%)	Deepfake Sophistication (%)	Detection Gap (%)
2019	65	40	-25
2020	72	55	-17
2021	78	70	-8
2022	82	82	0
2023	86	90	-4
2024	89	94	-5
2025	91	96	-5

Sources: Industry reports; academic detection benchmarks.

The data reveals that while detection accuracy has improved from 65% in 2019 to 91% in 2025, deepfake sophistication has grown from 40% to 96% in the same period. The gap, which narrowed in 2022, has widened again as diffusion models and transformer architectures have enabled increasingly convincing synthetic media.

Sectoral Distribution of Deepfake Fraud

Table 6: Global Deepfake Fraud Distribution by Sector (2023)

Sector	Percentage Share	Primary Attack Vector
Cryptocurrency	88%	Identity verification bypass, KYC fraud
Fintech	8%	Voice clone scams, document forgery
Media & Entertainment	2%	Reputational damage, disinformation
E-commerce	1%	Seller impersonation, review manipulation
Government	1%	Document forgery, impersonation

Source: SumsuB, Global Deepfake Fraud Report, 2024.

The overwhelming concentration of deepfake fraud in the cryptocurrency sector (88%) reflects the sector's reliance on remote identity verification and the irreversibility of blockchain transactions. However, as fintech and government services increasingly digitize, these sectors face escalating vulnerability.

India's Digital Infrastructure Readiness

Table 7: India Digital Infrastructure Readiness (Comparative Index)

Metric	India Score	Global Average	Gap
Internet Penetration	52	68	-16
Smartphone Users	95	88	+7
Social Media Users	48	62	-14
AI Startups	75	85	-10
Cybercrime Reporting	35	55	-20

Sources: TRAI; IAMAI; NASSCOM; World Bank Data.

India's relatively low cybercrime reporting score (35 vs. global average 55) is particularly concerning, suggesting significant underreporting of synthetic media offences. This underreporting may stem from stigma associated with NCII, lack of awareness about legal remedies, or distrust of law enforcement response.



Comparative Analysis: India in The Global Regulatory Landscape

The European Union: The AI Act Approach

The European Union's Artificial Intelligence Act, 2024, represents the world's first comprehensive horizontal AI regulation. Key provisions relevant to synthetic media include Article 52 (transparency obligations for AI systems generating deepfakes), Article 53 (automatic event logging), and Article 6 (high-risk classification for biometric identification systems).²³

The EU approach emphasizes ex-ante risk assessment and conformity marking rather than India's ex-post takedown model. The DSA's 24-hour takedown timeline is significantly longer than India's 3-hour requirement, but the EU framework provides stronger procedural protections, including Trusted Flagger mechanisms and transparency reporting obligations that India's Rules largely lack.²⁴

China: The Proactive Prohibition Model

China's regulatory approach to deepfakes is among the most restrictive globally. The Provisions on the Management of Deep Synthesis Internet Information Services, effective January 2023, require real-name registration for all users of deep synthesis services, mandatory labelling of all deep synthesis content, prohibition of using deep synthesis technology to produce prohibited content, and content review obligations on service providers.²⁵

China's framework is stricter than India's in requiring real-name verification but less specific on technical labelling standards. The absence of judicial independence in China means that enforcement is primarily administrative rather than judicial.

Singapore: The POFMA Framework

Singapore's Protection from Online Falsehoods and Manipulation Act, 2019 (POFMA), empowers ministers to issue correction directions and access blocking orders for online falsehoods. While not specifically targeting deepfakes, POFMA's broad definition of 'false statement of fact' encompasses synthetic media misinformation. The 24-hour compliance timeline and ministerial discretion have attracted criticism from human rights organizations.²⁶

United States: The Fragmented Approach

The United States lacks comprehensive federal legislation on synthetic media. The DEEPFAKES Accountability Act has been introduced in Congress multiple times but has not been enacted. Executive Order 14110 on Safe, Secure, and Trustworthy AI (October 2023) directs federal agencies to establish standards for AI-generated content authentication but does not create private rights of action or platform obligations. State-level legislation varies widely, with California, Texas, and Virginia enacting deepfake-specific laws primarily targeting NCII and electoral manipulation.

Table 8: Comparative Regulatory Stringency Index

Jurisdiction	Framework	Takedown Speed	Labelling Mandate	Criminal Penalties	Platform Liability	Overall Score
India	IT Rules, 2026	3 hours	10% visual/audio	Yes (up to 7 years)	Loss of safe harbour	92

China	Deep Synthesis Provisions	Immediate	Mandatory	Yes	Strict	85
EU	AI Act + DSA	24 hours	Machine-readable metadata	Yes (varies)	Graduated	78
Singapore	POFMA	24 hours	Correction directions	Yes	Ministerial	70
UK	Online Safety Bill	24 hours	Risk assessment-based	Yes	Ofcom-enforced	68
USA	Executive Order 14110	48+ hours	Voluntary standards	Limited state laws	Section 230 shield	45

Source: Author's analysis based on statutory provisions and regulatory documents.

Critical Gaps and Emerging Challenges

The Enforcement Capacity Deficit

India's regulatory framework, while ambitious on paper, faces a severe enforcement capacity deficit. The 3-hour takedown requirement presupposes:

1. **24/7 Content Moderation Teams:** Major platforms must maintain round-the-clock teams capable of reviewing and acting on takedown notices within 180 minutes. For platforms serving India's linguistic diversity (22 scheduled languages), this requires multilingual moderation capacity that currently does not exist at scale.
2. **Technical Detection Infrastructure:** The requirement to deploy 'reasonable and appropriate technical measures, including automated tools' presupposes access to detection technology that can identify synthetic media with acceptable error rates. Current detection accuracy of approximately 91% means 9% of content will be misclassified—either permitting harmful content or censoring legitimate expression.
3. **Law Enforcement Digital Literacy:** The requirement that police intimations must be issued by officers not below the rank of Deputy Inspector General (DIG) introduces a significant bottleneck. India's police force has approximately 1,000 DIG-rank officers for a population of 1.4 billion—an insufficient number to handle the volume of synthetic media complaints.

The 'Reasonable Technical Measures' Ambiguity

Rule 3(3)(a)(i) requires intermediaries to deploy 'reasonable and appropriate technical measures' to prevent prohibited SGI, but the standard remains undefined. No performance benchmarks, acceptable error-rate thresholds, or certification mechanisms have been specified. This ambiguity creates compliance uncertainty, enforcement arbitrariness, and potential innovation chill in Indian AI markets.

Cross-Border Jurisdiction Challenges

Many synthetic media applications—particularly those generating NCII—operate from jurisdictions outside India with weak or non-existent extradition treaties. The embedding of metadata identifiers at the point of generation is technically feasible only for tools within India's regulatory reach. Foreign platforms that do not maintain Indian subsidiaries may fall outside effective enforcement.

Free Expression Concerns

The broad definition of SGI and the 10% labelling requirement raise significant free expression concerns. Satirical content, political parody, and artistic expression using AI tools may be inadvertently captured. The Bombay High Court's decision in *Kunal Kamra v. Union of India*, 2024 SCC OnLine Bom 3052, striking down the Fact-Checking Unit amendment as ultra vires, signals judicial willingness to scrutinize content regulation mechanisms for constitutional compliance.

The proviso to Rule 4(1A)—deeming SSIMs that 'knowingly permit, promote or fail to act upon' SGI as having failed due diligence—creates a potent incentive for over-censorship. Platforms may err on the side of removal to avoid losing safe harbour protection, potentially suppressing legitimate speech.

The Metadata Conundrum

The requirement to embed 'permanent unique metadata identifiers' faces significant technical and practical challenges: (1) Metadata stripping: Standard image and video processing tools routinely strip metadata during compression, format conversion, and social media upload; (2) Encryption barriers: End-to-end encrypted platforms like WhatsApp cannot technically embed or verify metadata without breaking encryption; (3) Circumvention: Sophisticated users can employ tools to remove or alter metadata identifiers.

The Path Forward: A Proposed Reform Agenda

Legislative Reforms

1. Enact a Dedicated Synthetic Media Act: India should consider enacting a dedicated Synthetic Media Act that consolidates and expands upon the fragmented provisions currently scattered across the IT Act, BNS, POCSO, and IRWA. Such legislation should define synthetic media with precision, establish a tiered penalty structure, create a statutory right to 'digital integrity,' provide for statutory damages and attorney fee awards, and establish a statutory safe harbour for platforms implementing certified detection and labelling systems.
2. Amend the IT Act to Include Specific Deepfake Provisions: While the IT Rules, 2026, provide regulatory detail, they operate under the delegated legislation framework of Section 87. Primary legislation should explicitly criminalize the creation of non-consensual intimate deepfakes regardless of distribution, the use of deepfakes for electoral manipulation during designated campaign periods, the deployment of voice clones for financial fraud, and the creation of synthetic child sexual abuse material.
3. Strengthen POCSO for Synthetic CSEAM: The POCSO Act should be amended to explicitly address AI-generated child sexual abuse material, closing any ambiguity about whether synthetic content falls within the Act's scope. The amendment should clarify that synthetic CSEAM is treated identically to recorded CSEAM for sentencing purposes, establish mandatory reporting obligations for platforms detecting synthetic CSEAM, and create a dedicated fund for victim support and counseling.

Institutional Reforms

1. Establish a National Deepfake Detection Unit: Building upon the IISc Bengaluru and Infibeam Avenues partnership announced in 2024, India should establish a National Deepfake Detection Unit (NDDU) under MeitY with a mandate to develop national standards for deepfake detection technology, certify detection tools for platform compliance, provide technical assistance to law enforcement, maintain a national repository of verified deepfake incidents, and coordinate with international partners on cross-border investigations.²⁷
2. Enhance Judicial Capacity: The Supreme Court and High Courts should establish specialized digital benches with technical advisors proficient in AI and machine learning, fast-track procedures for NCII and synthetic media cases, standardized injunction templates for emergency relief, and training programs for district judges on digital evidence and synthetic media forensics.

3. **Strengthen Law Enforcement Digital Capabilities:** The Indian Cyber Crime Coordination Centre (I4C) should be expanded with dedicated synthetic media investigation cells in each state, access to advanced detection and attribution tools, liaison officers in key foreign jurisdictions, and regular training programs on evolving synthetic media technologies.

Platform Accountability Mechanisms

1. **Mandatory Transparency Reporting:** SSIMs should be required to publish quarterly transparency reports specifically addressing synthetic media, including number of SGI items detected and actioned, breakdown by category, average response time for takedown requests, appeals and reversals data, and geographic and linguistic distribution of synthetic media.
2. **Victim Notification and Support:** Platforms should be required to notify victims within 24 hours of detecting NCII depicting them, provide access to takedown request mechanisms with simplified procedures, offer referral information to victim support services, and preserve evidence for law enforcement without requiring victim-initiated legal process.
3. **Algorithmic Audit Requirements:** Platforms deploying recommendation algorithms that amplify synthetic media should undergo annual independent audits assessing the rate at which synthetic media is recommended to users, the demographic distribution of synthetic media exposure, the effectiveness of detection and labelling systems, and compliance with IT Rules, 2026, obligations.

International Cooperation

1. **Bilateral and Multilateral Agreements:** India should negotiate bilateral agreements with key jurisdictions (United States, European Union, United Kingdom, Singapore, United Arab Emirates) providing for mutual recognition of takedown orders, expedited evidence sharing in synthetic media investigations, joint training programs for law enforcement and regulators, and harmonized labelling and metadata standards.
2. **Participation in Global Standards Development:** India should actively participate in international standards development through the Coalition for Content Provenance and Authenticity (C2PA), the Partnership on AI, ISO/IEC JTC 1/SC 42 (Artificial Intelligence), and the Global Partnership on Artificial Intelligence (GPAI).

Public Awareness and Digital Literacy

1. **National Synthetic Media Literacy Campaign:** A sustained public awareness campaign should be launched, modeled on the European Union's 'Check. Recheck. Vote.' campaign, with components including school curricula incorporating synthetic media literacy, public service announcements in vernacular languages, partnerships with social media influencers for awareness messaging, and toolkits for identifying common deepfake indicators.²⁸
2. **Victim Support Infrastructure:** A national victim support hotline and online portal should be established, providing immediate emotional support and counseling referrals, step-by-step guidance for reporting to platforms and law enforcement, legal aid referrals for civil remedies, and reputation management resources.

CONCLUSION

The emergence of synthetic media represents a paradigmatic shift in the relationship between technology, truth, and law. India's response through the IT Rules, 2026, demonstrates both ambition and urgency—the 3-hour takedown timeline and 10% labelling requirement are unprecedented globally. Yet, as this article has demonstrated, regulatory ambition alone cannot overcome the structural challenges of enforcement capacity, cross-border jurisdiction, and the fundamental tension between harm prevention and free expression.

The empirical data presented in this study paints a sobering picture. The global deepfake AI market is projected to grow from USD 764.8 million in 2024 to USD 19.82 billion by 2033. Deepfake fraud surged ten-fold between

2022 and 2023. In India, 47% of respondents report direct or indirect victimization by AI voice scams, and detected deepfake content has grown 550% since 2019. Against this backdrop, the IT Rules, 2026, while necessary, are insufficient.

The judicial response through personality rights injunctions has provided meaningful relief to celebrity litigants but has not addressed the structural vulnerability of ordinary citizens. The comparative analysis reveals that India's framework is among the most stringent globally but lacks the procedural safeguards and transparency mechanisms of the EU approach and the technical specificity of China's provisions.

The reform agenda proposed in this article—encompassing a dedicated Synthetic Media Act, a National Deepfake Detection Unit, enhanced judicial capacity, mandatory platform transparency, and international cooperation—represents an integrated approach to what is fundamentally an integrated problem. Synthetic media does not respect jurisdictional boundaries, statutory silos, or institutional mandates. Effective governance requires similarly boundary-spanning responses.

As Justice D.Y. Chandrachud observed in Justice K.S. Puttaswamy, privacy is 'the constitutional core of human dignity.' The synthetic media revolution threatens that dignity in ways that the framers of our Constitution could not have imagined but would surely have recognized. The task before India's legal system is to ensure that the digital mirror reflects reality rather than algorithmic fabrication—and that when fabrication occurs, the law provides swift, effective, and just remedies.²⁹ The IT Rules, 2026, are a beginning, not an end. The true measure of India's regulatory success will not be the stringency of its rules but the effectiveness of their implementation, the accessibility of their remedies, and the balance they strike between security and liberty in an age of synthetic reality.³⁰

Table of Authorities

Cases

Amitabh Bachchan v. Rajat Nagi, CS (COMM) 493/2022 (Delhi High Court).

Anil Kapoor v. Simply Life India, CS (COMM) 652/2023 (Delhi High Court).

Jackie Shroff v. The Peppy Store, CS (COMM) 389/2024 (Delhi High Court).

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Kunal Kamra v. Union of India, 2024 SCC OnLine Bom 3052.

R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.

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

Statutes

Bharatiya Nyaya Sanhita, 2023, §§ 318, 319, 354, 356 (India).

Information Technology Act, 2000, §§ 66C, 66D, 66E, 67, 67A, 69A, 79, 87 (India).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (India).

Indecent Representation of Women (Prohibition) Act, 1986, § 3 (India).

Protection of Children from Sexual Offences Act, 2012, § 14 (India).

Representation of the People Act, 1951 (India).

Regulations and Official Documents

Ministry of Electronics and Information Technology, Frequently Asked Questions on IT Rules, 2021 (Amendment) (2026).

Ministry of Electronics and Information Technology, Explanatory Note on Proposed Amendments to IT Rules, 2021 (October 22, 2025).

Election Commission of India, Advisory on Use of AI and Deepfakes in Elections (2024).

REFERENCES

1. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Rule 2(1)(wa) (India).
2. Ian Goodfellow et al., Generative Adversarial Networks, 3 COMM. ACM 1392 (2020).
3. Grand View Research, Deepfake AI Market Size, Share & Trends Analysis Report (2025).
4. Fortune Business Insights, Deepfake Technology Market Size, Share | Growth Report [2034] (2025).
5. World Economic Forum, Global Risks Report 2024 (2024).
6. Sumsub, Global Deepfake Fraud Report (2024).
7. McAfee, AI Voice Scam Survey: India Results (2023).
8. Industry regulatory submissions to MeitY (2024) (on file with author).
9. Telecom Regulatory Authority of India, Indian Telecom Services Performance Indicators (2024).
10. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
11. Information Technology Act, 2000, § 79 (India).
12. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
13. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
14. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (India).
15. MeitY, Frequently Asked Questions on IT Rules, 2021 (Amendment) (2026).
16. R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
17. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
18. Amitabh Bachchan v. Rajat Nagi, CS (COMM) 493/2022 (Delhi High Court).
19. Vaish Law Associates, India IT Rules Before and After Amendment & AI-Generated Content (Feb. 10, 2026).
20. Market.us, Deepfake Detection Market Size | CAGR of 47.6% (2025).
21. Regulation (EU) 2024/1689, Artificial Intelligence Act (2024).
22. Regulation (EU) 2022/2065, Digital Services Act (2022).
23. Provisions on the Management of Deep Synthesis Internet Information Services (China), effective Jan. 10, 2023.
24. Protection from Online Falsehoods and Manipulation Act, 2019 (Singapore).
25. Human Rights Watch, Singapore's POFMA: A Threat to Free Expression (2020).
26. IISc Bengaluru and Infibeam Partner for Deepfake Detection, THE HINDU (2024).
27. European Commission, Check. Recheck. Vote. Campaign (2024).
28. Mondaq, India's New Deepfake Regulation: MeitY Notifies Amendments (Feb. 16, 2026).

APPENDIX: FIGURES

1. The following figures accompany this article and are available as supplementary materials:
2. Figure 1: Synthetic Media & Deepfake Landscape—Empirical Analysis (Four-panel figure showing Global Deepfake AI Market Size, Global Deepfake Detection Market, Regional Market Share, and India Deepfake Technology Market Projection).
3. Figure 2: Deepfake Misuse Patterns & Regulatory Response in India (Four-panel figure showing Deepfake Fraud Distribution by Sector, AI Voice Scam Impact in India, Takedown Timeline Comparison, and Detected Deepfake Content Growth Index).
4. Figure 3: Indian Legal Framework—Statutory Provisions & Judicial Response (Four-panel figure showing Maximum Imprisonment Under Applicable Statutes, Regulatory Timeline, Prohibited SGI Categories, and IT Rules 2026 Compliance Timelines).
5. Figure 4: Comparative Regulatory Analysis & Technology Response (Four-panel figure showing Regulatory Stringency Index, Deepfake Technology Market Share by Type, Detection Accuracy vs. Sophistication, and India Digital Infrastructure Readiness).