KING STUBB & KASIVA
ADVOCATES AND ATTORNEYS

TECHNOLOGY LAW & AI REGULATION

India's New IT Rules on Synthetic Media

A Comprehensive Legal Analysis

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026

February 2026

Gazette Notification G.S.R. 120(E) |Notified: 10 February 2026 | Effective: 20 February 2026

EXECUTIVE SUMMARY

The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified on 10 February 2026, represent India's first dedicated statutory framework for regulating AI-generated and synthetically altered media. This article undertakes a granular, clause-by-clause analysis examining doctrinal implications, compliance architecture, constitutional dimensions, global comparisons with the EU AI Act and C2PA standards, enforcement mechanisms, and strategic recommendations for intermediaries, AI developers, and policymakers.

20 Feb 2026	3 Hours	10%
Effective Date	New Takedown Window	Labelling Threshold

Contents

SECTION I

Introduction: From Platform Liability to Synthetic Reality

TheInformationTechnology (Intermediary Guidelines and Digital Media EthicsCode) Amendment Rules, 2026 (the "**2026 Amendment**"), notified vide Gazette Notification G.S.R. 120(E) on 10 February 2026, represent one of the most consequential shifts in India's digital regulatory architecture since the 2021 Intermediary Rules. For the first time, Indian law squarely addresses the phenomenon of AI-generated and synthetically altered media through an explicit statutory framework.

> ***Law is no longer only reactive to content harms; it is now anticipatory of technological capabilities. The 2026 Amendment regulates how content is created, not merely what content is posted.***

While earlier iterations of the Intermediary Rules focused on unlawful content, traceability, grievance redressal, and platform due diligence, the 2026 Amendment moves into a fundamentally new domain. It draws India into a growing global conversation that includes the EU AI Act's transparency obligations under Article 50, the United States' TAKE IT DOWN Act of 2025, China's mandatory AI labelling regulations effective September 2025, and Denmark's proposed amendments treating individual likeness as intellectual property.

The regulatory urgency is well-founded. India has witnessed a sharp escalation in deepfake-related harms: from the viral deepfake video of film actor Rashmika Mandanna in 2023, to AI voice-cloning fraud targeting business executives, to manipulated political videos during the 2024 general elections. Around a tenth of complaints to Rati's national helpline now involve deepfakes or AI-manipulated sexual imagery, with many women responding by withdrawing from online spaces altogether.

This article, prepared by King Stubb & Kasiva, undertakes a clause-by-clause analytical reading of the Amendment and examines its doctrinal implications, compliance architecture, constitutional dimensions, global comparisons, enforcement mechanisms, and strategic recommendations for platforms, AI developers, and digital content creators operating in India.

SECTION II

Short Title and Commencement: Why Dates Matter

TheAmendmentexplicitly statesthatitcomesinto forceon 20 February 2026,providinga mere ten-day window from notification to enforcement. Legally, commencement dates are critical in three respects.

1. **Compliance Windows.** Intermediaries receive virtually no transition period. This signals acute regulatory urgency around deepfakes and AI misuse. Platforms that have not already invested in synthetic media detection infrastructure face an immediate compliance deficit.

2. **Retrospective Liability Avoidance.** By fixing a future enforcement date, the government avoids claims of retrospective regulatory burden, a constitutional safeguard that protects existing lawful activity from being penalized under newly enacted rules.

3. **Signal to Courts.** Courts interpreting these rules will likely read them as a response to an emerging technological risk environment, granting regulators interpretive leeway in enforcement actions.

SECTION III

Foundational Definition: "Audio, Visual or Audio-Visual Information"

TheAmendmentintroduces an expansive definition encompassing 'any audio, image,photograph, graphic, video, moving visual recording, sound recording or any other audio, visual or audio-visual content, with or without accompanying audio, whether created, generated, modified or altered through any computer resource.' This definition is deliberately medium-agnostic and future-proof.

The language '**created, generated, modified or altered**' ensures that the rule captures both original and derivative works. Even minimal digital involvement brings content within scope. This forecloses the argument that only 'AI-native' content is regulated.

> **Key Takeaway:** Platforms cannot evade compliance by arguing that content is only 'edited' rather than 'generated.' The definition is deliberately inclusive to prevent regulatory arbitrage across content formats and media types.

SECTION IV

Core Innovation: "Synthetically Generated Information" (SGI)

The definition of SGI,codified undernew Rule 2(1)(wa),is the intellectual heart ofthe Amendment. SGI is defined 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.***'

Sentence-by-Sentence Analysis

"Artificially or algorithmically created." This covers generative AI models, neural networks, diffusion models, GANs, and rule-based automation. The law is technologically neutral, ensuring it does not become obsolete as AI capabilities evolve.

"Appears to be real, authentic or true." The test is perceptual, not technical. What matters is user perception, assessed through a 'reasonable person' standard. This is consistent with consumer protection doctrine but introduces subjectivity that may prove difficult to operationalize at scale.

"Indistinguishable from a natural person or real-world event." This creates a deception-focused threshold that mirrors emerging global definitions and directly targets deepfakes used for political manipulation, financial fraud, non-consensual intimate imagery, and defamation.

SECTION V

Carve-Outs: Protecting Legitimate Digital Activity

The proviso carefully excludes three categories of digital activity from the SGI definition:

(a) Routine Editorial Activities

- Good-faith editing, formatting, enhancement, and technical corrections
- Colour adjustment, noise reduction, transcription, and compression
- Activities that do not materially alter substance, context, or meaning

(b) Professional Content Creation

- Documents, presentations, PDF files, and educational or training materials
- Research outputs with illustrative, hypothetical, draft, or template-based content
- Content that does not result in false documents or electronic records

(c) Accessibility Improvements

- Use of computer resources solely for improving accessibility, clarity, and quality
- Translation, description, searchability, and discoverability enhancements
- Without generating, altering, or manipulating material parts of underlying information

Each carve-out deploys the language of **good faith** and **absence of material distortion**. This is constitutionally essential to avoid overbreadth challenges under Article 19(1)(a). Without such carve-outs, nearly all digital content could be classified as synthetic.

> **Policy Insight:** AI practitioners, including the Internet Freedom Foundation and The Fifth Elephant, have argued during public consultations that these carve-outs remain insufficiently precise. Image compression, brightness correction, phone camera filters, autocorrect suggestions, and translation tools risk being swept into the regulatory net.

SECTION VI

Expansion of 'Information' to Include SGI

New Rule 3(1A) clarifies that references to 'information' in unlawful contexts throughout the Intermediary Rules now include SGI. This integration is architecturally elegant: by riding on existing legal triggers rather than creating a parallel enforcement regime, SGI is automatically subject to every provision concerning unlawful content, intermediary due diligence, and grievance mechanisms. Courts will treat deepfakes as ordinary unlawful information once harm is demonstrated, eliminating separate jurisdictional arguments.

> **Litigation Forecast:** This provision closes a significant loophole. Prior to this amendment, platforms could argue that deepfakes fell outside the existing regulatory framework. That argument is no longer available.

SECTION VII

Safe Harbour Clarification and Technology Mandates

The rules clarify that removal or disabling of SGI in compliance with due diligence obligations does not violate Section 79(2) safe harbour conditions. This resolves a longstanding legal ambiguity. Platforms often hesitated to act aggressively against content for fear of being characterized as 'editorial' actors, which would strip safe harbour protection. By explicitly protecting proactive SGI removal, the Amendment encourages assertive content moderation.

Technology Mandate Strengthening

The Amendment replaces the previous discretionary language ('***endeavour to deploy technology-based measures***') with a mandatory obligation ('**deploy appropriate technical measures**'). This linguistic shift converts what was previously a best-efforts standard into a binding compliance requirement. The qualifier 'appropriate' suggests a reasonableness standard, but may be challenged if technically infeasible.

SECTION VIII

Periodic User Notification Duties

Intermediaries must inform users **at least once every three months** in a 'simple and effective manner' through rules, privacy policies, or user agreements about:

- **Immediate Enforcement Rights:** The platform's right to terminate or suspend access, remove or disable non-compliant content, or both
- **Legal Consequences:** Users may face penalties under the IT Act, 2000, punishment under applicable laws, and criminal prosecution where violations constitute offences
- **Mandatory Reporting:** Where violations involve reportable offences under the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) or the Protection of Children from Sexual Offences Act, 2012 (POCSO)

The language options under the Eighth Schedule (22 languages) localize compliance for India's linguistic diversity. This transforms user awareness from a one-time notice to an ongoing compliance obligation.

SECTION IX

Special Duties for SGI-Enabling Platforms

Intermediaries offering computer resources that enable synthetic content creation must additionally inform users of a comprehensive liability matrix. Creating synthetic content in violation of the rules may attract punishment under:

- Information Technology Act, 2000
- Bharatiya Nyaya Sanhita, 2023 (India's new criminal code)
- POCSO Act, 2012
- Representation of the People Act, 1951
- Indecent Representation of Women (Prohibition) Act, 1986
- Sexual Harassment of Women at Workplace Act, 2013
- Immoral Traffic (Prevention) Act, 1956

Consequences include immediate disabling of access, suspension or termination of user accounts without vitiating evidence, disclosure of the violator's identity to the complainant (where the complainant is the victim), and mandatory reporting to authorities for specified offences.

> **Regulatory Philosophy:** This provision targets not just ***hosts*** of content but ***tools of creation***. This is analogous to dual-use technology regulation in export control regimes. The comprehensive liability matrix extends beyond the IT Act to encompass election law, women's protection legislation, and criminal law.

SECTION X

Expeditious Action on Awareness

Upon knowledge or receipt of complaints, intermediaries must act 'swiftly' to address SGI-related content. This reinforces the 'actual knowledge' standard articulated by the Supreme Court in ***Shreya Singhal v. Union of India*** (2015) but tightens operational expectations considerably. Platforms can no longer rely on procedural delays or claim ignorance once a complaint has been filed.

SECTION XI

Drastically Reduced Timelines

The Amendment dramatically compresses compliance timelines across all critical categories:

Compliance Action	Previous	New	Reduction
Government/Court orders	36 hours	3 hours	92%
Urgent content removal	24 hours	2 hours	92%
Grievance redressal	15 days	7 days	53%
Grievance acknowledgment	24 hours	2 hours	92%

The 3-hour compliance window for government orders represents an 83% reduction from the previous 36-hour standard. Intermediaries must comply with orders from authorized officers (not below Deputy Inspector General of Police rank) within three hours of receipt.

> **Constitutional Concern:** These timelines may face challenges under Article 14 (equality and reasonableness). The compressed windows limit intermediaries' ability to verify orders, seek legal consultation, or file appeals. They may lead to over-compliance and erroneous removal of legitimate content.

SECTION XII

Due Diligence for SGI: Prohibited Content Categories

Platforms enabling SGI creation must deploy 'reasonable and appropriate technical measures, including automated tools or other suitable mechanisms' to prevent creation of content across four prohibited categories:

Category 1: Exploitative and Obscene Content

- Child Sexual Exploitative and Abuse Material (CSEAM)
- Non-consensual intimate imagery
- Obscene, pornographic, or paedophilic content; content invasive of bodily privacy

Category 2: False Documents

- Content resulting in the creation of false documents or false electronic records

Category 3: Security Threats

- Content relating to preparation, development, or procurement of explosive materials, arms, or ammunition

Category 4: Deceptive Impersonation

- Content falsely depicting natural persons or real-world events by misrepresenting identity, voice, conduct, action, or statement
- Content depicting events as having occurred in a manner likely to deceive

Category 4 directly targets deepfakes used for political manipulation, financial fraud, revenge pornography, defamation, and election interference. This provision effectively mandates **AI policing AI**, pushing the industry toward watermarking, provenance tracking, and detection models.

SECTION XIII

Mandatory Labelling, Metadata, and Provenance

For synthetic content that is permitted but not prohibited, the Amendment introduces precise labelling and metadata requirements:

Visual Content

Labels must ensure prominent visibility. For visual content, the label must cover **at least 10% of the total surface area**.

Audio Content

Audio must be prominently prefixed with a disclosure constituting **at least the first 10% of the total duration**.

Technical Provenance

Platforms must embed **permanent metadata** including a **unique identifier** that identifies the computer resource used. Intermediaries shall NOT enable modification, suppression, or removal of labels, metadata, or identifiers.

> **Global Context:** This transparency regime aligns with the EU AI Act's Article 50 obligations and C2PA (Coalition for Content Provenance and Authenticity) standards. However, India lacks the EU's layered, risk-based classification. Metadata fragility remains a challenge: screenshots, re-encoding, and compression can strip embedded provenance.

SECTION XIV

Enhanced Obligations for Significant Social Media Intermediaries (SSMIs)

SSMIs (platforms exceeding 5 million registered users in India) face enhanced obligations through a mandatory **three-step verification process**:

1. **User Declaration.** Require users to declare whether uploaded content is synthetically generated.
2. **Technical Verification.** Deploy 'reasonable and appropriate technical measures' including automated tools to verify the accuracy of declarations.
3. **Labelling.** Where declaration or verification confirms synthetic origin, ensure content is clearly and prominently labelled.

Strict Liability Standard

Where an SSMI knowingly permits, promotes, or fails to act upon synthetic content violations, it will be **deemed to have failed its due diligence obligations**, risking loss of safe harbour protection under Section 79. This creates a quasi-strict liability regime where actual knowledge triggers mandatory action and willful blindness is not a defence.

SECTION XV

Alignment with the Bharatiya Nyaya Sanhita, 2023

The Amendment replaces all IPC references with the Bharatiya Nyaya Sanhita, 2023 (BNS), effective 1 July 2024. India replaced its colonial-era criminal law with three new statutes: the BNS (substantive criminal law), the Bharatiya Nagarik Suraksha Sanhita, 2023 (criminal procedure), and the Bharatiya Sakshya Adhiniyam, 2023 (evidence law).

Key BNS provisions relevant to synthetic media:

- **Section 336:** Forgery for harming reputation, with enhanced clarity on digital forgery and impersonation
- **Section 353:** Penalizes false or misleading statements causing public mischief or fear
- **Section 356:** Criminal defamation with improved provisions for online content (up to 2 years)
- **Section 111:** Organized cybercrimes, covering coordinated deepfake campaigns
- **Section 77:** Criminalizes non-consensual intimate imagery, directly relevant to deepfake pornography
- **Section 316:** Cheating through misleading digital information, applicable to deepfake-enabled fraud

The BNS's expanded definition of 'document,' explicitly including electronic records and digital content, provides a stronger prosecutorial foundation for deepfake-related offences.

SECTION XVI

Constitutional and Policy Reflections

1. Article 14: Equality and Reasonableness

The compressed response timelines may be challenged as unreasonable and arbitrary. They may be impossible for smaller intermediaries and discriminatory in impact. The State may counter-argue exigency of harmful content justifies rapid response.

2. Article 19(1)(a): Freedom of Speech and Expression

Mandatory labelling may be challenged as compelled speech. Pre-publication verification could constitute prior restraint. The absence of explicit exemptions for satire, parody, journalism, and artistic expression remains a vulnerability. The Supreme Court's proportionality framework in ***Puttaswamy*** and ***Modern Dental College*** requires restrictions to be necessary, least restrictive, and proportionate.

3. Article 21: Right to Privacy

Metadata embedding and provenance tracking create surveillance-capable infrastructure. While aimed at transparency, these mechanisms could be repurposed for tracking creators of politically inconvenient but lawful content.

4. Procedural Due Process

The 3-hour window is insufficient for legal review or appeals. Precedents from ***Shreya Singhal*** (2015), ***Anuradha Bhasin*** (2020), and ***Facebook India v. Union of India*** (2021) will be central to judicial review.

5. Regulatory Architecture

Civil society organizations have raised concerns about concentration of rulemaking, enforcement, and adjudicatory functions within MeitY without independent review mechanisms, creating risks of arbitrary enforcement.

SECTION XVII

Global Comparative Analysis

India's Amendment arrives at a moment of global regulatory convergence:

Jurisdiction	Framework	Approach	Key Difference
European Union	AI Act (2024/1689) + DSA	Risk-based classification; graduated obligations	Longer timelines; more procedural safeguards

United States	Section 230 CDA + TAKE IT DOWN Act	Platform self-regulation; state-level patchwork	Stronger intermediary immunity; lighter regulation
United Kingdom	Online Safety Act 2023	Duty of care; Ofcom enforcement	Focus on systems; 12-18 month rollout
China	Deep Synthesis Regulations (2023)	Mandatory watermarks; real-name registration	Both prescriptive; China broader AI governance scope
India	2026 IT Rules Amendment	Prescriptive; platform responsibility; rapid timelines	Most aggressive timelines; broadest liability matrix

India's approach is notably more prescriptive and punitive than most democratic jurisdictions. While the EU classifies systems by risk and links obligations accordingly, India treats all synthetically generated content as inherently suspect. India also lacks the graduated implementation timelines (up to 36 months) available under the EU regime.

SECTION XVIII

Implementation Roadmap and Compliance Strategy

Phase 1: Immediate (By 20 February 2026)

- Update terms of service and privacy policies to reflect new obligations
- Begin quarterly user notification cycles
- Establish 3-hour government order response capability and 2-hour grievance acknowledgment

Phase 2: Short-term (By June 2026)

- Deploy synthetic media detection and labelling infrastructure
- Implement user declaration and verification workflows
- Deploy metadata embedding and provenance tracking systems

Phase 3: Medium-term (By December 2026)

- Monitor constitutional challenges and court rulings
- Establish industry best practices; participate in standards consortiums

Estimated Compliance Costs

Platform Size	Detection Systems	Operations	Total Estimate
Large (SSMIs)	$10-50M	$5-20M/yr	$15-70M+
Medium	$1-10M	$500K-5M/yr	$1.5-15M
Small/Startup	May be prohibitive	Outsourcing reqd.	Exit risk

SECTION XIX

Regulatory Philosophy: From Neutrality to Responsibility

The 2026 Amendment marks a decisive philosophical shift. Intermediaries are no longer positioned as passive conduits entitled to safe harbour protection merely by maintaining a hands-off posture. They are reconceived as **governance actors** with affirmative obligations to detect, label, moderate, and report synthetic content.

> ***The 2026 Amendment does not merely regulate content. It regulates capability, imposing obligations not just on what platforms host, but on what their tools enable.***

This reconceptualization borrows from financial services regulation, environmental compliance, and dual-use technology export controls: domains where entities are held responsible not just for their actions but for the capabilities they make available.

SECTION XX

Conclusion: A New Era of Synthetic Media Law

The 2026 Amendment is India's most comprehensive attempt to regulate AI-generated media within a binding legal framework. It arrives at a moment of global regulatory convergence and contributes distinctively to the international conversation.

Key Contributions

1. A precise legislative definition of synthetically generated information, codified as Rule 2(1)(wa)
2. Mandatory labelling with quantified visibility standards (10% thresholds for visual and audio content)
3. Permanent metadata and provenance requirements aligned with global C2PA standards
4. Dramatically compressed compliance timelines (3-hour and 2-hour windows)
5. Expanded platform due diligence covering both hosting and creation tools
6. A comprehensive liability matrix extending across criminal, election, women's protection, and technology law
7. Full integration with the Bharatiya Nyaya Sanhita's modernized criminal law framework

Critical Assessment

Strengths: The Amendment addresses a genuine and growing threat. Its comprehensive coverage, clear obligations, and alignment with criminal law reforms represent a serious regulatory effort. The carve-outs for legitimate digital activity demonstrate thoughtful drafting.

Vulnerabilities: The compressed timelines may be operationally impossible. Detection technology remains imperfect. There is a real risk of chilling legitimate speech and innovation, overblocking through false positives, and disadvantaging smaller platforms. Limited procedural safeguards remain a constitutional concern.

> ***The regulatory question is no longer whether to regulate deepfakes, but how to do so without sacrificing innovation, privacy, and free expression at the altar of content control. The next 12-24 months will be decisive.***

The world will watch India's experiment closely. If successful in curbing harms while preserving innovation and rights, it may chart a path for democratic AI governance. If it falters through overreach, it may serve as a cautionary tale. Stakeholders must engage constructively to ensure India's synthetic media framework serves its legitimate objectives while respecting digital rights essential to a vibrant democracy.

Key Statutory References

- **Primary:** IT Act, 2000 (21 of 2000); BNS, 2023 (45 of 2023); BNSS, 2023 (46 of 2023); POCSO Act, 2012 (32 of 2012)
- **Related:** Representation of the People Act, 1951; Indecent Representation of Women (Prohibition) Act, 1986; Sexual Harassment of Women at Workplace Act, 2013; Explosive Substances Act, 1908
- **Constitutional:** Articles 14, 19(1)(a), 19(2), and 21
- **Notifications:** G.S.R. 139(E) (25.02.2021); G.S.R. 794(E) (28.10.2022); G.S.R. 275(E) (06.04.2023); G.S.R. 120(E) (10.02.2026)

KING STUBB & KASIVA
ADVOCATES AND ATTORNEYS

Authors & Contributors

Himanshu Deora
Partner

Sindhuja Kashyap
Partner

Aniket Ghosh
Partner

Vivek Boray
Partner

Our Offices Across India

New Delhi
RNM Tower, 5th Floor, Metro Pillar No. 331,
i4, B1, NH-19, Mohan Cooperative
Industrial Estate, New Delhi - 110044
info@ksandk.com

Mumbai - Nariman Point
Office No. 61, 6th Floor,
Atlanta Building, Jamnalal Bajaj Road,
Nariman Point, Mumbai - 400021
mumbai@ksandk.com

Mumbai - Andheri (West)
802, 8th Floor, REMICOMMERCIO,
Shah Industrial Estate, Veera Desai Road,
Andheri (West), Mumbai - 400053
mumbai@ksandk.com

Hyderabad
404,Shangrila Plaza, Road No. 2,
Banjara Hills, Opp. KBR Park,
Hyderabad - 500034
hyderabad@ksandk.com

Pune
Bootstart Cowork, First Floor,
Arcadian Building, Plot No. 12,
Koregaon Park, Pune - 411001
pune@ksandk.com

Bengaluru
1A, Lavelle Mansion,
1/2, Lavelle Road,
Bengaluru - 560001
bangalore@ksandk.com

Mumbai - Lower Parel
301A, 3rd Floor,Piramal Towers,
Peninsula Corporate Park, Senapati
Bapat Marg, Lower Parel, Mumbai - 400013
mumbai@ksandk.com

Chennai
211,Alpha Wing, Second Floor,
Raheja Towers, #177, Anna Salai,
Chennai - 600002
chennai@ksandk.com

Kochi
1stFloor, Manavalan Building,
Amulya Street, Banerji Road,
Ernakulam, Kochi - 682018
kochi@ksandk.com

Mangalore
Office No.406, 4th Floor,
Ajanta Business Center, Kapikad,
Bejai, Mangalore - 575004
mangalore@ksandk.com