INDIALAW

CYBER LAW

IT Rules 2026 Corporate Playbook: Practical Roadmap for Synthetic Information Regulation

AUTHOR Appurv Bhatia

PUBLISHED 14 February 2026

A Comprehensive Analysis of the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026

Executive Summary

The Ministry of Electronics and Information Technology has issued landmark amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 or IT Rules 2026, introducing comprehensive regulations governing synthetically generated information, commonly known as deepfakes and AI-generated content. These amendments, notified on February 10, 2026, and effective from February 20, 2026, impose stringent obligations on intermediaries, particularly social media platforms, with significant compliance, reporting, and liability implications.

Table of contents

I. Introduction and Legislative Context

The Central Government, exercising powers under Section 87(1) and clauses (z) and (zg) of Section 87(2) of the Information Technology Act, 2000, has enacted these amendments through notification G.S.R. 120(E). This regulatory intervention addresses the growing concerns around AI-generated content that can be indistinguishable from authentic media, posing risks to national security, public order, individual privacy, and democratic processes.

The amendments represent India's proactive stance in regulating emerging technologies while balancing innovation with public safety and individual rights.

II. Key Definitions and Scope

A. Audio, Visual or Audio-Visual Information

The amendments introduce a comprehensive 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."

B. Synthetically Generated Information

The Rules define "synthetically generated information" as audio, visual, or audio-visual information that is:

- Artificially or algorithmically created, generated, modified, or altered using computer resources
- Appears to be real, authentic, or true
- Depicts or portrays any individual or event in a manner that is, or is likely to be, indistinguishable from a natural person or real-world event

C. Exclusions from Definition

The following activities are specifically excluded from the definition of synthetically generated information:

1. **Routine Editing:** Good-faith editing, formatting, enhancement, technical correction, color adjustment, noise reduction, transcription, or compression that does not materially alter the substance, context, or meaning of the underlying content
2. **Professional Content Creation:** Routine creation of documents, presentations, PDF files, educational materials, and research outputs using illustrative, hypothetical, draft, template-based, or conceptual content, where such creation does not result in false documents or false electronic records
3. **Accessibility Improvements:** Use of computer resources solely for improving accessibility, clarity, quality, translation, description, searchability, or discoverability, without generating, altering, or manipulating any material part of the underlying information

D. Expanded Scope of "Information"

Critically, any reference to "information" in the context of unlawful acts now includes synthetically generated information, unless the context requires otherwise. This expansion applies to violations under Rule 3(1)(b), Rule 3(1)(d), and Rules 4(2) and 4(4).

III. Enhanced Due Diligence Obligations for All Intermediaries

A. Periodic User Notifications

All intermediaries must now inform users **at least once every three months** (increased from ad-hoc notifications) in a simple and effective manner through their terms of service, privacy policies, or user agreements, in English or any language specified in the Eighth Schedule of the Constitution, regarding:

1. **Termination Rights:** The intermediary's right to immediately terminate or suspend user access or remove non-compliant information in case of violations
2. **Legal Liability:** That non-compliance relating to unlawful creation, generation, modification, hosting, uploading, publishing, transmitting, or disseminating of information may result in penalties or punishment under the IT Act or other applicable laws
3. **Mandatory Reporting Obligations:** Where violations constitute offenses under laws such as the Bharatiya Nagarik Suraksha Sanhita, 2023 or the Protection of Children from Sexual Offences Act, 2012 that require mandatory reporting, such offenses will be reported to appropriate authorities

B. Expedited Takedown Timelines

The amendments significantly reduce response times for intermediaries:

Action Required	Previous Timeline	New Timeline
Court order or government directive response	36 hours	3 hours
Remove or disable (Serious nature, nudity, sexual act)	24 hours	2 hours
Grievance disposal	15 days	7 days
Removal of information	72 hours	36 hours

C. Written Authorization Requirement

Government orders for content removal must now be issued by an authorized officer **through a written order**. For police administration, authorized officers must be of the rank of Deputy Inspector General of Police or above, specifically authorized by the appropriate government.

IV. Special Obligations for Intermediaries Offering Synthetic Media Generation Tools

A. Prohibited Content Categories

Intermediaries offering computer resources that enable creation of synthetically generated information must deploy reasonable and appropriate technical measures, including automated tools, to prevent generation of content that:

1. **Child Sexual Abuse Material:** Contains child sexual exploitative and abuse material, non-consensual intimate imagery, or is obscene, pornographic, paedophilic, or invasive of another person's privacy
2. **False Documents:** Results in creation, generation, modification, or alteration of any false document or false electronic record
3. **Dangerous Materials:** Relates to preparation, development, or procurement of explosive material, arms, or ammunition
4. **Misleading Impersonation:** Falsely depicts or portrays a natural person or real-world event by misrepresenting identity, voice, conduct, action, statement, or events in a manner likely to deceive, with or without the person's involvement

B. Mandatory Labeling and Metadata Requirements

For all synthetically generated content not prohibited under the above categories, intermediaries must ensure:

- **Prominent Labeling:** Content must be prominently labeled to ensure visibility in visual displays that is easily noticeable and adequately perceivable
- **Audio Disclosure:** For audio content, a prominently prefixed audio disclosure must identify the content as synthetically generated
- **Permanent Metadata:** Content must be embedded with permanent metadata or technical provenance mechanisms, including a unique identifier, to identify the computer resource used for generation

- **Anti-Tampering:** Intermediaries must not enable modification, suppression, or removal of labels, metadata, or unique identifiers

C. Enhanced User Warnings

Intermediaries must additionally inform users that violations may result in:

- Immediate disabling of access or content removal
- Suspension or termination of user accounts without vitiating evidence
- Disclosure of violating user's identity to complainants who are victims
- Reporting to appropriate authorities where violations constitute criminal offenses under various laws including:
  - Bharatiya Nyaya Sanhita, 2023
  - Protection of Children from Sexual Offences 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

D. Proactive Monitoring Obligations

Intermediaries must take expeditious action upon becoming aware of violations through:

- Self-initiated detection
- Receipt of actual knowledge
- Grievances, complaints, or information received under the Rules

V. Additional Obligations for Significant Social Media Intermediaries

Significant social media intermediaries face heightened compliance requirements under the new Rule 4(1A):

A. Pre-Publication Requirements

Before displaying, uploading, or publishing any information, such intermediaries must:

1. **User Declaration:** Require users to declare whether information is synthetically generated
2. **Technical Verification:** Deploy appropriate technical measures, including automated tools, to verify the accuracy of user declarations, considering the nature, format, and source of information
3. **Mandatory Display:** Where declarations or technical verification confirm synthetic generation, ensure clear and prominent display with appropriate labels or notices

B. Liability for Non-Compliance

Intermediaries that knowingly permit, promote, or fail to act upon synthetically generated information in violation of these rules shall be deemed to have **failed to exercise due diligence**, potentially losing safe harbor protections under Section 79 of the IT Act.

C. Strengthened Proactive Content Filtering

The amendment changes the language from intermediaries shall "endeavour to deploy" to shall "**deploy** appropriate technical measures" for identifying previously removed content, making proactive filtering mandatory rather than aspirational.

VI. Safe Harbor Clarifications

A. Preservation of Intermediary Protection

The amendments clarify that removal of, or disabling access to, any information (including synthetically generated information, data, or communication links) by an intermediary in compliance with these Rules shall **not** amount to a violation of conditions under Section 79(2)(a) or 79(2)(b) of the IT Act.

This clarification provides legal certainty that compliance-driven content moderation will not jeopardize intermediary status.

B. Deployment of Automated Tools

Use of automated tools and appropriate technical measures for compliance is explicitly recognized and protected, addressing previous ambiguity about the use of algorithmic content moderation.

VII. Updated Legal References

The amendments update references from the Indian Penal Code to the **Bharatiya Nyaya Sanhita, 2023**, reflecting the recent criminal law reforms in India.

VIII. Corporate Compliance Roadmap

Immediate Actions Required (By February 20, 2026)

1. **Policy Updates:** Revise terms of service, privacy policies, and user agreements to incorporate new definitions and obligations
2. **User Notifications:** Implement quarterly notification mechanisms to inform users of compliance requirements and consequences
3. **Technical Infrastructure:** Assess and upgrade technical measures for:
    1. Detection of synthetically generated content
    1. Automated content filtering
    1. Labeling and metadata embedding systems
    1. User declaration collection mechanisms
4. **Response Systems:** Reconfigure complaint handling and government order response systems to meet new timelines (3 hours, 2 hours, 7 days)
5. **Training Programs:** Conduct comprehensive training for:
    1. Content moderation teams
    1. Grievance officers
    1. Legal and compliance personnel
    1. Product and engineering teams
6. **Documentation:** Establish robust documentation systems for:
    1. User declarations
    1. Verification processes
    1. Takedown actions
    1. Reporting to authorities

Medium-Term Strategic Measures

1. **AI/ML Investment:** Invest in sophisticated AI and machine learning systems for:
    1. Deepfake detection
    1. Synthetic media identification
    1. Pattern recognition for prohibited content categories
2. **Third-Party Audits:** Engage independent auditors to assess compliance with technical measures and due diligence requirements
3. **Industry Collaboration:** Participate in industry forums to develop standardized approaches to synthetic media labeling, metadata protocols, and verification mechanisms
4. **Legal Advisory:** Retain specialized legal counsel for:
    1. Interpretation of “reasonable and appropriate technical measures”
    1. Safe harbor protection strategies

1. Government liaison and regulatory engagement

IX. Risk Assessment and Mitigation

A. Compliance Risks

Risk Category	Potential Exposure	Mitigation Strategy
Inadequate technical measures	Loss of safe harbor, liability for user-generated content	Deploy state-of-art detection tools, document reasonable efforts
Delayed response to orders	Penalties, regulatory action	Implement 24/7 compliance teams, automated alert systems
Improper labeling	User deception claims, regulatory scrutiny	Standardized labeling protocols, quality assurance checks
Over-blocking	User complaints, reputation damage	Balanced approach, appeals mechanism

B. Operational Challenges

- **Technical Feasibility:** Current AI detection technology has limitations in identifying sophisticated deepfakes
- **False Positives:** Risk of incorrectly flagging legitimate content as synthetic
- **Volume Management:** Large-scale platforms must process millions of pieces of content daily
- **International Operations:** Reconciling India-specific requirements with global content policies

C. Recommended Mitigation Approaches

- Implement layered detection approaches combining automated tools and human review
- Maintain detailed logs demonstrating “reasonable and appropriate” efforts
- Establish clear internal escalation procedures for edge cases
- Create user-friendly appeals processes for disputed classifications
- Engage with regulatory authorities for clarifications and guidance

X. Impact on Business Models and Product Development

A. Social Media Platforms

- Must implement pre-publication verification and labeling systems
- Face increased operational costs for compliance infrastructure
- May experience reduced user-generated content volume due to declaration requirements
- Need to redesign user interfaces to accommodate labeling and disclosure mechanisms

B. AI Content Generation Tools

- Must embed permanent metadata and unique identifiers in all outputs
- Cannot enable creation of prohibited content categories
- Face potential liability if tools are misused despite reasonable safeguards
- May need to implement usage restrictions and monitoring

C. E-Commerce and Marketplace Platforms

- Must address synthetic product images and manipulated reviews
- Need verification mechanisms for seller-uploaded content
- Face challenges in applying rules to commercial versus user-generated content

D. Enterprise Communication Platforms

- Must balance compliance with business confidentiality and privacy
- Need clear policies on internal versus external communications

- May require separate treatment for enterprise versus consumer offerings

XI. Enforcement and Penalties

While the amendment Rules themselves do not specify new penalties, non-compliance exposes intermediaries to:

1. **Loss of Safe Harbor:** Failure to exercise due diligence results in loss of protection under Section 79 of the IT Act, exposing intermediaries to liability for third-party content
2. **Criminal Liability:** Potential prosecution under:
    1. Bharatiya Nyaya Sanhita, 2023
    1. IT Act, 2000 (Sections 66, 66C, 66D, 66E, 67, 67A, 67B)
    1. Protection of Children from Sexual Offences Act, 2012
3. **Regulatory Action:** Ministry of Electronics and IT may issue directions under Section 69A of the IT Act for blocking of non-compliant platforms
4. **Civil Liability:** Exposure to damages claims from individuals harmed by synthetic media that platforms failed to address
5. **Reputational Damage:** Public disclosure of compliance failures can significantly impact brand value and user trust

XII. International Comparisons and Global Implications

India's approach aligns with, and in some aspects exceeds, regulatory frameworks in other jurisdictions:

- **European Union:** The Digital Services Act and AI Act contain similar provisions on synthetic media labeling and platform obligations
- **United States:** Multiple state laws (e.g., California AB 602, Texas SB 751) address deepfakes, but no comprehensive federal framework exists
- **China:** Internet Information Service Deep Synthesis Management Provisions (2022) impose similar labeling and registration requirements
- **Singapore:** Online Criminal Harms Act (2024) addresses synthetic media in context of criminal content

Multinational platforms must now reconcile India's requirements with varying obligations across jurisdictions, potentially leading to adoption of highest common denominator approaches globally.

XIII. Pending Clarifications and Industry Concerns

Several aspects require further regulatory guidance:

A. Technical Standards

- What constitutes "reasonable and appropriate technical measures" given evolving technology?
- Are there approved or certified detection tools that satisfy compliance?
- How should platforms handle uncertainty in detection outcomes?

B. Metadata Specifications

- What format should permanent metadata take?
- How should unique identifiers be structured?
- Are there interoperability standards with other jurisdictions?

C. Exclusion Interpretations

- How broadly should "routine editing" be interpreted?
- When does enhancement cross into material alteration?
- How are borderline cases involving multiple edits treated?

D. Enforcement Mechanisms

- How will the Ministry assess compliance with due diligence obligations?
- Will there be a grace period for implementation of technical measures?

- What documentation must platforms maintain to demonstrate compliance?

XIV. Recommendations for Corporate Boards and Senior Management

1. **Board Oversight:** Establish board-level oversight of synthetic media compliance, given potential magnitude of liability exposure
2. **Risk Committee Review:** Include synthetic media regulations in enterprise risk management frameworks
3. **Budget Allocation:** Approve adequate budgets for compliance infrastructure, recognizing this as business-critical investment
4. **Cross-Functional Teams:** Create dedicated task forces involving legal, technical, product, policy, and communications functions
5. **External Engagement:** Authorize participation in industry associations and regulatory dialogues to shape implementation guidance
6. **Scenario Planning:** Conduct tabletop exercises for handling high-profile synthetic media incidents
7. **Insurance Review:** Assess adequacy of cyber liability and directors & officers insurance for synthetic media-related claims
8. **Vendor Management:** Ensure third-party service providers (cloud, content moderation, AI tools) support compliance requirements
9. **Regular Audits:** Institute quarterly compliance audits with findings reported to senior management and board
10. **Public Positioning:** Develop proactive public communications strategy on platform approach to synthetic media

XV. Conclusion

The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, represent a paradigm shift in India's approach to regulating digital intermediaries and synthetic media. The regulations impose comprehensive, prescriptive obligations that will require significant operational, technical, and financial investments from affected platforms.

Key takeaways for the corporate world:

- **Immediate action is required:** The February 20, 2026 effective date leaves minimal time for implementation
- **Compliance is not optional:** Loss of safe harbor protections represents existential risk for intermediary business models
- **Technical sophistication is mandatory:** "Reasonable efforts" will be measured against deployment of state-of-art detection and labeling systems
- **Documentation is critical:** Platforms must maintain comprehensive records demonstrating due diligence
- **Collaboration is beneficial:** Industry-wide approaches to technical standards and best practices will facilitate compliance

As India emerges as one of the world's largest digital markets, these regulations will significantly influence both domestic and international platform operations. Companies must treat compliance not as a legal checkbox, but as a core business imperative requiring senior leadership attention, adequate resourcing, and ongoing commitment.

Organizations that proactively embrace these requirements and invest in robust compliance frameworks will not only mitigate regulatory risk but also build user trust in an era of increasingly sophisticated synthetic media.

References

[1] Ministry of Electronics and Information Technology. (2026, February 10). Notification G.S.R. 120(E) – Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. https://www.meity.gov.in

For more details, write to us at contact@indialaw.in

Related Practice Areas

Information Technology