INDIA'S FIRST STEP TOWARD AI REGULATION: NEW IT RULES AMENDMENTS

TRACE LAW PARTNERS

On February 10, 2026, the Government of India through the Ministry of Electronics and Information Technology ("**MeitY**") introduced amendments to the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code Rules, 2021* ("**IT Rules**"), effective from **February 20, 2026 ("Amendments")** to regulate synthetically generated information ("**SGI**") online, and tighten takedown and grievance redressal timelines for intermediary platforms, amongst others.[i] Non-compliance with the IT Rules, including the Amendment, may result in loss of safe harbour by intermediary platforms, i.e., immunity from liability for user-generated content.[ii]

01

The Amendments were introduced in the run-up to the Government of India's flagship AI Summit 2026, where one of the key principles emphasized was the development and deployment of safe and trusted AI. They also followed a judicial trend of multiple injunction orders issued against AI-generated content, including deepfakes and synthetic media that impersonated or misrepresented public figures and private individuals.[iii] Most recently, a social media platform in India came under heavy scrutiny from MeitY following AI-generated obscene content of women by its AI tool.

02

The Amendments mark India's first step towards horizontal AI regulations, by introducing a regulatory framework for a certain type of AI-generated content, SGI, being audio, visual, or audio-visual deepfake-type content. Broadly, the Amendments prohibit certain forms of SGI and introduce labelling requirements for lawful SGI. However, significant uncertainty persists around how platforms will distinguish between the two forms of SGI and implement labelling obligations in practice. The Amendments also do not distinguish between different types of AI platforms, ranging from AI providers, deployers, etc., and aim to bucket every platform on which AI-generated content is available into a single category and regulate them uniformly as intermediaries.

03

The Amendments were accompanied by FAQs which stated that they were introduced to regulate SGI in view of deepfakes, misinformation, non-consensual intimate imagery ("**NCII**"), child sexual abuse material ("**CSAM**"), and other unlawful content capable of misleading users, violating privacy or threatening national integrity.[iv] However, the scope of the Amendments extends beyond SGI, and they enhance several existing obligations applicable to intermediaries. Most notably, the Amendments drastically reduce timelines to act upon takedown requests from 36 hours to 3 hours[v], as well as grievance redressal[vi], whilst empowering additional authorities to issue takedown requests.[vii] The Amendments also impose enhanced user awareness and accountability obligations.[viii]

04

Whilst the Amendments followed a draft version circulated for public comments in October 2025, several obligations introduced in the final version were not included in the October draft.[ix] These provisions were therefore not included in the consultative process. Following the Amendments, key intermediary platforms, including social media platforms, have pushed back on the Amendments. Latest reports suggest that MeitY is not inclined to entertain a dilution of obligations.[x]

REDUCTION IN TIMELINES FOR TAKEDOWN AND GRIEVANCE REDRESSAL

The timelines for grievance redressal and takedown upon being informed by a court, or authorized Government agencies, have been reduced as follows:

OBLIGATION	PREVIOUS TIMELINE	REVISED TIMELINE
Takedown upon intimation by a court or by reasoned intimation from an authorized Government agency[xi]	36 hours	3 hours To illustrate, the FAQs provide that if a reasoned intimation is received from an appropriate Government agency at 11 AM to disable access to a deceptive SGI video, the intermediary must comply by 2 PM at the latest.
Resolution of complaints sent to the grievance redressal officer[xii]	15 days	7 days
Resolution of complaints relating to more serious offences such as harassment, invasion of privacy, gambling or money laundering, content creating religious enmity, against Indian sovereignty or public order, pornographic content, pedophilic content, amongst others[xiii]	72 hours	36 hours
To take reasonable measures to disable NCII content, impersonation, or artificially morphed content[xiv]	24 hours of receipt of a complaint by a victim or a person on their behalf	2 hours of receipt of complaint by a victim or a person on their behalf

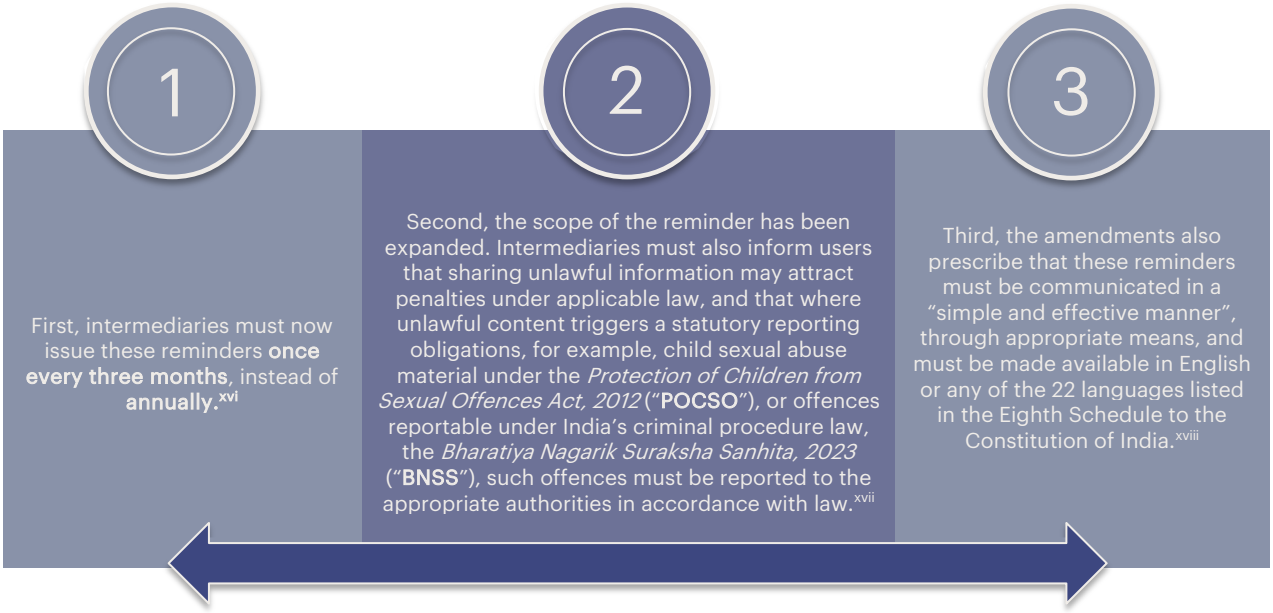
TLP Comment:

- The reduction in timelines for take down apply to *all* categories of unlawful content, and not just SGI. With the appointment of additional authorised officers to issue takedown requests, platforms can expect higher volumes of takedown requests.
- These amendments did not feature in the draft Amendments released in October, and hence platforms did not have the ability to prepare for compliance or account for these changes during the consultative process.
- These Amendments have been the subject of heavy industry pushback, given that platforms typically take takedown decisions based on legal analysis, involving the determination of the procedural requirements of a request being met, as well as the illegality of content itself.
- Platforms may rely on automated takedown more heavily to meet deadlines, which may result in a chilling effect on free speech where takedown is affected without appreciation of the nuances of satire, parody, lawful criticism, and the like. Implementation of this obligation requires 24-hour, round-the-clock readiness by moderation teams to meet these deadlines.

SHORTENED TIMELINES FOR USER REMINDERS; ENHANCED USER AWARENESS OBLIGATIONS:

Under the IT Rules, intermediaries are required to inform users at least once every three months that non-compliance with the platform's terms and conditions may result in consequences such as suspension or termination of access to the service, or removal of non-compliant content.[xv] The IT Rules did not previously prescribe any language requirements for such reminders.

The amendments introduce several changes:



The accompanying FAQs further clarify that platforms may comply by periodically displaying or sending advisories (every three months) informing users that unlawful content, including deepfakes, NCII and CSAM, is prohibited, that violations may lead to removal of content or suspension/termination of accounts, and that certain offences may be reported to law enforcement authorities.[xix]

TLP Comment:

- The obligation to remind users of reporting obligations in relation to CSAM appears to stem from a push from the National Commission for Protection of Child Rights (NCPCR) to enforce reporting requirements for CSAM content by intermediaries under the POCSO. The Supreme Court emphasized the mandatory nature of reporting obligations by intermediaries under POCSO and had emphasized that intermediaries could not claim safe harbour under Section 79, unless they complied with such reporting requirements in the landmark judgment of *Just Rights for Children Alliance v. S. Harish* (2024 SCC OnLine SC 2611).
- This increased frequency of such user reminders is likely to result in notification fatigue, and in fact may result in such notifications being overlooked by users.
- The language requirements are also likely to be cumbersome for global platforms, and platforms may consider practical solutions instead of providing such reminders in all 22

OBLIGATIONS IN RELATION TO SYNTHETICALLY GENERATED INFORMATION ("SGI")

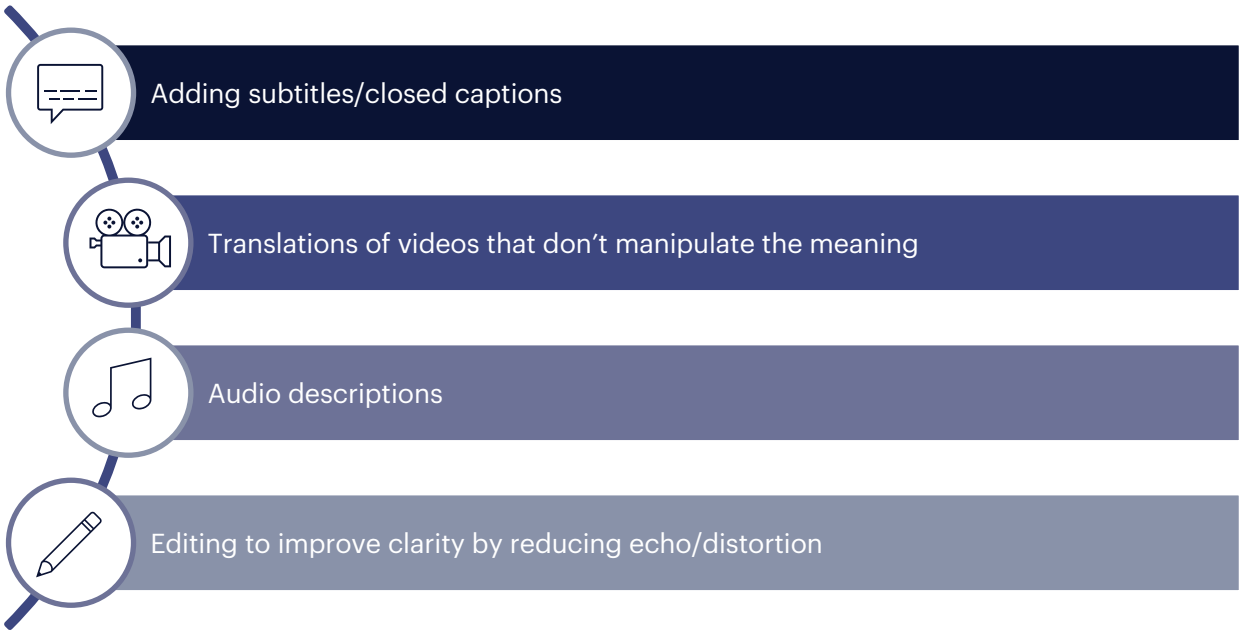
The Amendments introduce a definition of SGI[xx], and several new obligations in relation to SGI, including labelling requirements and preventive measures to preclude prohibited SGI.

Scope of SGI

As per the definition, SGI refers to audio, visual, or audiovisual content created, modified, or altered using computer resources so that it appears real or authentic, and depicts a person or event in a way that is likely to be perceived as indistinguishable from a real person or real-world event. However, certain types of good-faith editing and other functions are excluded from this definition.

The definition of SGI is also limited to synthetically generated "*audio, visual, or audiovisual information*"[xxi], **excluding text content**. However, the FAQs clarify that where SGI is accompanied by text, the text is still subject to general compliances under the IT Rules.[xxii] For instance, an SGI video of a bomb blast accompanied by text content that perpetuates the deception ("*a bomb blast took place today*") may be subject to takedown obligations under the IT Rules.

Following concerns that the definition of SGI under the draft Amendments covered even innocuous editing apps, the Amendments specifically exclude 'routine or good faith' editing, formatting, etc., and editing to improve accessibility, quality, etc. of content. The FAQs give further guidance on what is excluded from SGI[xxiii], including:



They also clarify that lawful creative uses of synthetic media, such as for satire or artistic purposes, may not be considered SGI, and may be permitted so long as they are appropriately labelled.[xxiv]

TLP Comment:

- The scope of SGI is limited to content which *appears* to be realistic people or events in a manner that deceives users into believing it is genuine, therefore limiting SGI to deepfakes-type content, and not AI-generated content generally. AI-generated melodies for instance, are likely excluded.
- A question arises as to whether AI-generated content which depicts virtual persons bearing no resemblance to real-world people falls within the scope of SGI. Arguably, given the intent of the Amendments to regulate deceptive content, such content is also included within the scope of SGI.

Which platforms are covered

The obligations in relation to SGI apply to intermediaries that enable or facilitate the creation, generation, modification, alteration, publication, transmission, sharing or dissemination of SGI.[xxv] The FAQs clarify that this may apply both to intermediaries offering AI image/video generation or editing tools, voice synthesis / voice cloning tools, as well as **platforms that facilitate the publication or dissemination of SGI.**[xxvi]

TLP Comment:

- The obligations in relation to SGI apply uniformly to platforms that both enable the creation of SGI and platforms that simply allow users to post content, which may include SGI**.** This is unlike contemporaneous legislation such as the EU's AI Act, that distinguish between AI providers that develop AI systems, AI users, and AI distributors. The Amendments also do not distinguish between different types of AI platforms, ranging from AI providers, deployers, etc., and aim to bucket every platform on which AI-generated content is available into a single category and regulate them uniformly as intermediaries.
- It appears that even intermediaries that do not enable the *creation* of SGI, but where SGI may be published, are subject to these obligations. This approach raises concerns, as it imposes preventive obligations on platforms that function primarily as passive conduits for user-generated content. The concept of intermediaries and safe harbour rests on the premise that intermediaries are not required to take preventive steps till such time as they receive actual knowledge. Requiring such platforms to take preventive measures blurs the distinction between publisher and intermediary platforms.
- A question arises as to whether platforms that enable the creation of SGI, i.e., AI generation platforms, are intermediaries in the first place in relation to such output. Under the IT Act, intermediaries are understood as entities that receive, transmit, or store user-generated content on their behalf. However, in the case of AI-generated platforms, the content is not merely transmitted or hosted on behalf of the user, but generated by the platform itself. Arguably, AI-generation platforms fall outside the definition of an intermediary.
- The lines are further blurred in the case of platforms that are social media intermediaries having an AI-generation functionality, such as platforms supporting AI-generated ad creation on the platform itself.

Preventive Obligations:

Intermediaries that allow users to create, publish, SGI must deploy *reasonable and technical measures* including automated tools or other suitable mechanisms to disallow users from creating, modifying, publishing any SGI that violates applicable law, including CSAM, NCII, misrepresents someone's identity or an event, create false documents, relates to the preparation or development of explosive material, arms or ammunition, is vulgar, indecent, or sexually explicit, amongst others[xxvii] ("**Prohibited SGI**").

TLP Comment:

- In their current form, this obligation raises several practical compliance issues for intermediaries.
- The scope of *reasonable and technical measures including automated tools* to disallow users from creating, etc., such SGI is unclear. The FAQs also do not shed light on the scope of this obligation, i.e., whether it requires automated detection tools even *prior* to the users posting such content.
- It is also unclear how intermediaries will make the determination of which SGI violates applicable law, and which SGI does not violate applicable law.
    - For instance, SGI of a celebrity created under license granted by the celebrity is not unlawful. It is unclear how intermediary platforms can make such determinations, that too even prior to such content being posted.
- Some illustrative categories of Prohibited SGI under this Amendment does not even appear to be illegal, for instance, content which is "vulgar" or "indecent."

Labelling Requirements:

The Amendments also introduce labelling requirements for SGI that is not Prohibited SGI[xxviii]:

- SGI must be prominently labelled in a manner that ensures clear visibility and is easily noticeable and adequately perceivable by users. In the case of visual content, the label must appear in the visual display, while audio content must include a prominently prefixed audio disclosure indicating that the information is synthetically generated.
- The disclosure must enable users to immediately identify that the information has been created, generated, modified or altered using a computer resource.
- In addition, to the extent technically feasible, the content must be embedded with permanent metadata or other appropriate technical provenance mechanisms, including a unique identifier, that can help identify the computer resource of the intermediary used to create, generate, modify or alter the information.

The Amendments also require that intermediaries must not enable the modification, suppression or removal of the visible labels, permanent metadata or any unique identifiers embedded in the content in accordance with the labelling requirements.[xxix] For instance, intermediaries must not offer a 'remove watermark' or 'export without metadata' functionality.

To illustrate: A lawful SGI AI-generated audio message (e.g., a synthetic voice narration for an awareness campaign or an audio announcement generated using text-to-speech), not covered under the Prohibited SGI should include a prominently prefixed audio disclosure such as *"This audio is synthetically generated*" at the beginning, and should also carry embedded permanent metadata / provenance mechanism, including a unique identifier, to enable identification of the audio as SGI and the computer resource used to generate/alter it.

TLP Comment:

- In the wake of the introduction of these obligations, several intermediary platforms have started rolling out labels for AI-generated content generally, including 'Made with AI' or 'Content Credential' labels.
- It is also unclear how certain types of SGI may be detected by intermediary platforms to trigger labelling. For instance, if a screenshot of SGI is sought to be uploaded, intermediary platforms may not be able to detect such content as SGI in the first place.
- It is unclear how intermediary platforms may identify permissible SGI, which is required to be labelled as well. For instance, the FAQs permit creative uses of synthetic media, such as for satire or artistic purposes, so long as they are appropriately labelled. However, it is unclear how intermediaries may make contextual determinations of whether SGI amounts to satire or not.

User Warnings:

Intermediaries must also inform users that[xxx]:

- Using the platform to create or publish SGI in contravention of the above conditions may attract penalty under applicable Indian law;
- It may additionally lead to removal of content, account suspension/termination, user identity disclosure to the complainant (victim) in accordance with law, and reporting of the user under laws requiring such reporting, such as POCSO.

To illustrate: A voice cloning tool must warn users that misuse for deception/impersonation may attract legal action.

- Intermediaries must take such expeditious and appropriate action (i.e., removal of content, suspension/termination, and identification of users) when it becomes aware, either of their own accord, or upon receipt of actual knowledge from the court/authorised officials, or on the basis of any grievance/complaint under the IT Rules. The FAQs clarify that platforms must also preserve the information (i.e., logs and other information) for evidentiary purposes in case of investigations.[xxxi]
- The Amendments clarify that removal of content, including SGI content, would not dilute
- intermediaries' immunity from liability for unlawful content (i.e., safe harbour).

TLP Comment:

- The requirement that intermediaries identify the user responsible for the violation and disclose the identity of such user to the complainant "in accordance with applicable law" raises practical and legal concerns. While intermediaries are required to inform users that their identity may be disclosed in the event of non-compliance, Indian law does not presently contain any general provision that obligates disclosing the personal details of one user directly to another private party. Requiring intermediaries to disclose the identity of an alleged violating user directly to the complainant appears to be inconsistent with the existing legal framework under the Digital Personal Data Protection Act, 2023.
- It is also unclear at what juncture the intermediary is expected to have awareness to take steps even if no court order or notification has been issued.

SGI DECLARATION OBLIGATIONS FOR SSMI

The Amendments require SSMIs that enable users to display, upload, or publish information to[xxxii]:

1. Declare whether such information is SGI prior to publication;
2. Deploy reasonable and proportionate technical measures to verify the accuracy of such declarations, having regard to the nature, format, and source of information; and
3. Where such a declaration/technical verification confirms that the information is SGI, ensure that it is clearly and prominently displayed as such. The explanation to this rule requires that SSMIs ensure that no SGI is published without such a declaration or label.

The FAQs clarify that the declarations must be verified by the SSMI *prior to publication.*[xxxiii]

SSMIs that become aware, or it is otherwise established that the intermediary knowingly permitted, promoted or failed to act upon such SGI in contravention of these rules would be deemed to have not fulfilled their due diligence obligations under the IT Rules.[xxxiv] The Amendments, therefore, appear to link an intermediary's knowledge or awareness of violating SGI to potential loss of compliance with the due diligence framework.

TLP Comment:

- Requiring users to declare whether each piece of content they upload is SGI, verify such declarations, and subsequently label the content as SGI move beyond intermediaries' passive role by effectively requiring platforms to introduce pre-publication compliance checks and content classification mechanisms within the publishing process. Implementation of these requirements would fundamentally change the way users interact with social media.
- It is unclear how the "awareness" or "knowledge" standard applicable to SSMIs would be interpreted in practice. As platforms increasingly rely on automated detection tools to identify potentially synthetic content, such tools may incorrectly flag content as possible SGI. It remains unclear whether the mere flagging of content by such technical systems would be treated as conferring awareness or knowledge on the intermediary. Technical detection signals, which are often prone to false positives and errors, should not be equated with legal awareness. Consistent with the nature of the intermediary liability framework established by Indian judgments, knowledge should ideally arise only upon the intermediary receiving actual knowledge, such as through a court order or a notification from the appropriate Government or its authorised agency.
- It is unclear how all types of SSMIs will practically enforce these declaration requirements in relation to all types of content:
    - For instance, on messaging platforms, user communications are often private, encrypted, and exchanged in real time between individuals or within small groups. Requiring a declaration as to whether each message, image, video, or audio file constitutes SGI prior to transmission may be operationally impractical.
    - Live content presents additional implementation challenges. Content is generated and transmitted instantaneously, leaving little opportunity for platforms to require a declaration, verify the accuracy of such a declaration, and apply labels before the content becomes visible to viewers.

MANDATORY DEPLOYMENT OF TECHNICAL MEASURES FOR *PROACTIVE* DETECTION

SSMIs were formerly required to *endeavour* to deploy appropriate technical measures to proactively identify certain types of unlawful information and take it down (such as CSAM, rape content, or content which has been previously disabled). The Amendments now *mandate* that SSMIs do so.[xxxv]

TLP Comment:

- While the previous obligation was in the nature of a best-efforts requirement, the Amendments now elevate it to a mandatory compliance standard.
- Given that automated detection tools may generate false positives, false negatives, and contextual errors, intermediaries may face practical challenges in implementing systems that both comply with the rule and minimise the risk of over-removal of legitimate content.

EFFECT OF NON-COMPLIANCE

Non-compliance with the obligations under the IT Rules, including these Amendments, may result in loss of safe harbour, i.e., loss of immunity from liability for unlawful user-generated content accorded to intermediary platforms under the IT Act.[xxxvi] The IT Rules state that non-observance with the rules may also result in liability for the intermediary under laws prohibiting certain content, such as India's criminal law, the Bharatiya Nyaya Sanhita, 2023 ("**BNS**").[xxxvii]

TLP Comment:

- While the IT Rules state that non-compliance with the rules could result in liability for the intermediary under laws such as the BNS, arguably non-compliance should not result in automatic liability on the intermediary platform. Imposition of criminal liability requires assessment of a variety of factors, including criminal intent in most cases, as well as causation between the accused's acts and the alleged offence.

[i] Available here: https://www.meity.gov.in/static/uploads/2026/02/f55fe52418b03f58b0669f6a8bc03b6d.pdf
[ii] Section 79, Information Technology Act, 2000 ("IT Act").
[iii] Aishwarya Rai Bachchan v. Aishwaryaworld.com, 2025 SCC OnLine Del 5943, Kamya Buch v. JIX5A, 2025 SCC OnLine Del 6428, Suniel V Shetty v. John Doe S Ashok Kumar, 2025 SCC OnLine Bom 3918
[iv] Available here: https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf
[v] Rule 3(1)(d), Information Technology (Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 ("IT Rules").
[vi] Rule 3(2)(a), IT Rules.
[vii] Rule 3(1)(d)(ii)(I), IT Rules.
[viii] Rule 3(1)(ca), IT Rules.
[ix] Available here: https://www.meity.gov.in/static/uploads/2025/10/9de47fb06522b9e40a61e4731bc7de51.pdf
[x] Available here: https://theprint.in/india/governance/govt-refuses-to-dilute-ai-content-rules-meeting-attended-by-google-meta-ends-in-30-mins-with-a-firm-no/2863878/
[xi] Rule 3(1)(d), IT Rules.
[xii] Rule 3(2)(a)(i), IT Rules.
[xiii] Rule 3(2)(a)(i), IT Rules.
[xiv] Rule 3(2)(b), IT Rules.
[xv] Rule 3(1)(c), IT Rules.
[xvi] Rule 3(1)(c), IT Rules.
[xvii] Rule 3(1)(c)(iii), IT Rules.
[xviii] Rule 3(1)(c), IT Rules.
[xix] FAQ No. 11, Frequently Asked Questions on The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 ("FAQs"). Available here: https://www.meity.gov.in/static/uploads/2025/10/065b6deb585441b5ccdf8be42502a49c.pdf
[xx] Rule 2(wa), IT Rules, 'synthetically generated information' means 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; Provided that the purposes of this clause, an audio, visual or audio-visual information shall not be deemed to be 'synthetically generated information', where such audio, visual or audio-visual information arises from–
(a) routine or good-faith editing, formatting, enhancement, technical correction, colour adjustment, noise reduction, transcription, or compression that does not materially alter, distort, or misrepresent the substance, context, or meaning of the underlying audio, visual or audio-visual information; or
(b) the routine or good-faith creation, preparation, formatting, presentation or design of documents, presentations, portable document format (PDF) files, educational or training materials, research outputs, including the use of illustrative, hypothetical, draft, template-based or conceptual content, where such creation or presentation does not result in the creation or generation of any false document or false electronic record; or

(c) the 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 audio, visual or audiovisual information;

[xxi] Rule 2(ca), IT Rules, 'audio, visual or audio-visual information' means 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;

[xxii] FAQ No. 8, FAQs.

[xxiii] FAQ No. 6, FAQs.

[xxiv] FAQ No. 7, FAQs.

[xxv] Rule 3(3), IT Rules.

[xxvi] FAQ No. 20, FAQs.

[xxvii] Rule 3(3)(a)(i), IT Rules.

[xxviii] Rule 3(3)(ii), IT Rules.

[xxix] Rule 3(3)(b), IT Rules.

[xxx] Rule 3(3), IT Rules.

[xxxi] FAQ No. 13, FAQs.

[xxxii] Rule 4(IA), IT Rules.

[xxxiii] FAQ No. 26, FAQs.

[xxxiv] Rule 4(IA), IT Rules.

[xxxv] Rule 4(4), IT Rules.

[xxxvi] Section 79, IT Act

[xxxvii] Rule 7, IT Rules.