

Regulating Deepfakes in India: Understanding the Draft Amendments and Their Implications

On October 22, 2025, the Ministry of Electronics and Information Technology (“MeitY”) released draft amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“Intermediary Rules”) (“Draft Amendments”) to address the harms posed by synthetically generated information (“SGI”)¹

As per the Explanatory Note to the Draft Amendments, the intent is to regulate deepfake content, misinformation, and other unlawful content capable of misleading users.² The Draft Amendments were introduced amidst concerns of deepfake content going viral on social media platforms, depicting individuals in acts or statements to carry out financial frauds, damage reputations, influencer elections, amongst others³.

These amendments have also been introduced amid criticism that existing laws, i.e., the Intermediary Rules, the Information Technology Act, 2000 (“IT Act”) and the Bharatiya Nyaya Sanhita, 2023 do not contain adequate provisions addressing deepfakes.

Background to the Draft Amendments

In the past few years, MeitY has repeatedly expressed its commitment to the issue of deepfakes, issuing multiple advisories to social media platforms to undertake due diligence obligations under the Intermediary Rules in relation to such content, or risk losing platform immunity under the IT Act.⁴

Public personalities and celebrities have increasingly approached Indian courts to protect their

¹ See: <https://www.meity.gov.in/static/uploads/2025/10/9de47fb06522b9e40a61e4731bc7de51.pdf>

² See: <https://www.meity.gov.in/static/uploads/2025/10/8e40cdd134cd92dd783a37556428c370.pdf>

³ Ibid.

⁴ Ministry of Electronics and Information Technology, Press Release, November 7, 2023, available at [https://pib.gov.in/PressReleaseFramePage.aspx?PRID=1975445#:~:text=%E2%80%9CFor%20those%20who%20find%20themselves.Minister%20said%20while%20summing%20up](https://pib.gov.in/PressReleaseFramePage.aspx?PRID=1975445#:~:text=%E2%80%9CFor%20those%20who%20find%20themselves.Minister%20said%20while%20summing%20up;); Ministry of Electronics and Information Technology, Press Release, December 26, 2023, available at <https://pib.gov.in/PressReleaseFramePage.aspx?PRID=1990542>.

personality rights against online deepfakes.⁵ Courts have expressed concern over the ease with which such content proliferates given the accessibility of AI tools, repeated uploads on rogue websites, and use of URL-redirection or identity-masking methods. Courts have provided relief in the form of injunctions restraining *John Doe* websites from using a celebrity's likeness for commercial gain without authorization (including through AI); directions to intermediaries such as ISPs and TSPs to block identified websites; directions to social-media platforms to remove infringing content and accounts within set timelines and compelling disclosure of subscriber information of those publishing such content. However, obtaining such relief remains time-consuming, and enforcement is complicated by "hydra-headed" websites that quickly resurface as mirrors with masked registration details.

In response to a public interest litigation before the Delhi High Court⁶ regarding the proliferation of deepfake technology, the court in November 2024, directed the Central Government to nominate members to a committee tasked with examining deepfake regulation. The committee was instructed to review foreign regulatory frameworks and consult relevant stakeholders, including intermediary platforms, telecommunication service providers, victims of deepfakes, and websites that create or deploy such content, and to submit its report to the Court. As per the status report filed before the Delhi High Court by the government ("**Status Report**"),⁷ the committee has reportedly held two meetings ("**Deepfake Committee Meetings**") during which discussions focused on AI detection tools, forensic analysis, watermarking, the accuracy and limitations of detection methods, and the synthetic media labelling policies of major technology companies. The committee had sought an extension until July 23, 2025 to submit its report before the court and has yet to file it. The case remains ongoing, and the Draft Amendments were released during its pendency.

Following the publication of the Draft Amendments, the Election Commission of India (ECI) issued an advisory on the responsible use of SGI during elections.⁸ In view of the growing use of AI-generated depictions of political leaders conveying electorally sensitive messages, and the potential impact of such content on the integrity of the electoral process and the conduct of free and fair elections, the ECI laid down specific directions for political parties, candidates, and campaign representatives.

The advisory mandates that all SGI used for campaigning be clearly labelled in the prescribed manner, and that the entities responsible for generating such content be prominently disclosed. It further requires that any unlawful SGI be taken down within three hours of detection or notice, and that political parties maintain internal records of all AI-generated campaign material, including creator details and timestamps - for verification by the ECI.

Draft Amendments

1. Definition of Synthetically Generated Information

The obligations proposed under the Draft Amendments apply to SGI. SGI is defined to mean "*information which is artificially or algorithmically created, generated, modified or altered using a computer resource, in a manner that such information reasonably appears to be authentic or true.*"

⁵ *Anil Kapoor v. Simply Life India & Ors* CS(Comm) 652/2023 and I.A. 18237/2023-18243/2023; *Arijit Singh v. Codible Ventures LLP*, 2024 SCC OnLine Bom 2445; *Sadhguru Jagadish Vasudev v. Igor Isakov*, 2025 SCC OnLine Del 3804

⁶ *Rajat Sharma v. Union of India* [WP (C) No. 6560 of 2024]; *Chaitanya Rohilla v. Union of India* [W.P.(C) 15596/2023]

⁷ See: <https://docs.google.com/viewerng/viewer?url=https://getapi.indiatvnews.com/doc/status-report-dated-24032025.pdf>

⁸ Advisory dated October 24, 2025

The Draft Amendments impose new declaration, labelling, identification and takedown requirements, amongst others, on intermediaries, particularly social media platforms in relation to SGI.

While the intent of the law is to regulate deepfakes, the broad scope of the definition may unintentionally bring within its impact even general information which is artificially edited or modified, such as a photo edited for brightness, or a video compressed, routine image or audio enhancements.

The threshold for '*reasonably appears to be authentic or true*' is also unclear, i.e., whether even artistic or satirical or parody content that is not misleading is subject to the above obligations. It is also unclear if it includes animated/stylized content or content other than realistic content, such as in augmented reality (AR) or virtual reality (VR) settings. In such a case, all computer-aided design in fields such as architecture, engineering, biology etc. may also be considered SGI for the purposes of the obligations such as labelling under the Intermediary Rules.

2. Removal of SGI does not affect safe harbour status:

The Draft Amendments clarify that intermediaries will not lose their safe harbour protection, i.e., immunity from liability for third party content under Sections 79(2)(a) and (b) of the IT Act for removing prohibited content under Rule 3(1)(b) of the Intermediary Rules. This includes content such as SGI. Rule 3(1)(b) requires intermediaries to take reasonable steps to ensure that certain types of prohibited information are not hosted on their platforms as part of their due diligence obligations.

This clarification reassures intermediaries that proactively removing prohibited content in good faith will not affect their safe harbour protection or exemption from liability for third-party information.

This was earlier provided in the proviso to Rule 3(1)(d) which clarified that the removal or disabling of access to information, data or communication links on a voluntary basis or on the basis of grievances, would not dilute their safe harbour. This proviso has been deleted by way of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025 notified on October 22, 2025.

3. Labelling of SGI created using intermediary platforms

Intermediaries that offer a computer resource which may "enable, permit, or facilitate" the creation, generation, modification, or alteration of information as SGI must clearly label such content with a permanent unique identifier or metadata (which cannot be removed or modified). The label must be visibly or audibly prominent - covering at least 10% of the visual area or the first 10% of audio duration - so users can immediately identify it as SGI created using the intermediary's platform. Intermediaries are prohibited from modifying, suppressing or removing such labels.

It appears the purpose of this provision is to require generative AI platforms on which SGI may be generated, created, modified, etc., to be subject to the labelling requirements. However, it is unclear whether such platforms qualify as intermediaries with respect to such features and hence are subject to the Intermediary Rules in the first place. For example, platforms that allow users to generate video or voice clones may not fall neatly within the definition of an 'intermediary,' since the core content is

produced autonomously by the system rather than merely transmitted or stored on behalf of a user. Intermediary platforms (such as social media platforms which have generative AI features on their intermediary offerings), however, would clearly fall within the ambit of this obligation.

It appears that the labelling obligation may also apply to AR/VR software.

Additionally, since the Draft Amendments do not distinguish between misleading deepfakes and harmless synthetic content such as parodies, animated filters, reenactments etc, such content will be required to be labelled in the same manner as misleading deepfakes. This would lead to over-labelling, diluting the intention behind a labelling requirement.

Further, as per the Status Report, during the Committee Meetings, BigTech platforms had highlighted the ease with which sophisticated actors can remove identifiers from AI-generated content. Hence, the labelling would need to be sufficiently advanced to prevent its removal.

4. SSMI's due diligence obligations and user declarations

Significant social media intermediaries (“SSMIs”), i.e., social media intermediaries with over 5 million registered users in India, are required to ensure the following prior to permitting upload of SGI on their platforms:

- (i) Users declare where content is SGI.
- (ii) SSMIs verify the accuracy of such user declarations, using reasonable and appropriate technical measures, including automated tools, considering the nature, format, and source of such information.
- (iii) If such information is confirmed as SGI, ensure that the content is clearly and prominently labelled as such.

If an SSMI becomes aware or knowingly permits or fails to act upon SGI, it would amount to a violation of its due diligence obligations.

It is to be noted that this obligation is limited to SSMIs and does not apply to other intermediary platforms (i.e., non-social media), and smaller social media and intermediary platforms, where such content may continue to be uploaded without appropriate declarations.

Even for SSMIs, however, there appear to be several practical difficulties with implementing this obligation.

It is unclear how the SSMI will *require* users to declare that the information is SGI prior to uploading every piece of content. Billions of posts, comments, and uploads are made daily. For SSMIs in the nature of instant messaging platforms, this does not appear to be practically possible at all. Additionally, it is unclear how this obligation would apply to livestreams or real-time content streaming which are not ‘uploads’. Finally, this obligation may not fully address the risk of misinformation among users who may not grasp the significance of the label, as deepfakes could still be shared even with a proper declaration in place.

It also does not appear possible for SSMIs to determine the accuracy of the declaration at all times. Platforms may have algorithmic tools to detect AI-generated patterns or anomalies, but these tools cannot verify the factual accuracy of the

underlying content at all times. During the Deepfake Committee Meetings, the challenges in accurately detecting deepfakes, especially when there are diversified Indian accents and audio-only content, were highlighted.

It is also unclear whether the obligation applies in the context of satirical content, comedic content which is clearly false, or subjective opinions.

It also remains unclear when exactly an intermediary is considered to have “awareness” of SGI, or has *‘knowingly permitted, promoted or failed to act upon’* SGI.

For instance, if a user submits a complaint alleging that certain content is SGI, it is uncertain whether this would automatically establish awareness on the part of the intermediary, or whether further verification, or multiple user complaints, would be required before the due diligence obligations are triggered. Further, it is unclear if the labelling obligation upon detection of SGI would have to match the labelling requirements under draft rule 3(3).

The Draft Amendments further clarify that the obligation of the SSMI is limited to taking reasonable and proportionate technical measures to ensure and verify user declarations. If undeclared SGI continues to be hosted on an SSMI platform despite such efforts, this will not amount to a violation of the SSMI’s due diligence obligations.

5. Existing obligations under the Intermediary Rules now applicable in relation to SGI

As per the Draft Amendments, any reference to ‘information’ under the Intermediary Rules, in the context of information being used to commit an unlawful act, including under clause (b) and (d) of sub-rule (1) of rule 3(1)(b), rule 3(1)(d), rule 4(2) and rule 4(4), should be construed to include SGI, unless the context otherwise requires.

Based on this, the following obligations also become applicable to intermediaries in relation to SGI:

- (i) **Due diligence obligations:** Intermediaries must make “reasonable efforts” to ensure that users do not upload, host, display, or share unlawful information as specified under Rule 3(1)(b); such obligations shall now also extend to SGI which falls within the categories of prohibited content. The scope of intermediaries’ obligation to take “reasonable efforts”, which now extends to SGI, has always been unclear. The extent of this obligation was the subject of the dispute in the case of Starbucks Corporation and Anr v. National Internet Exchange of India and Ors, CS (Comm) 224/2023, where the Delhi High Court held that there was no “guidance as to the actual scope and import” of the obligation, and it was “shrouded in obscurity” and is a “fertile ground for litigation and uncertainty”. Pursuant to the court’s direction, MEITY had submitted an affidavit to the court, attempting to provide certain guidance on the scope of this obligation. However, the scope of the obligation remains largely ambiguous.
- (ii) **Takedown obligations:** Intermediaries are required to remove or disable access to unlawful information, including SGI, pursuant to a court order or government direction under Rule 3(1)(d).

- (iii) **Preservation of records:** Intermediaries must preserve disabled information, including SGI, and related records for a period of 180 days for investigation purposes.
- (iv) **Compliance reporting:** Periodic compliance reports must include details of SGI to which access was disabled, including where such action resulted from proactive monitoring or detection.
- (v) **Advertising and promotion of SGI:** SSMLs that promote or provide SGI for direct financial benefit - by increasing its visibility, prominence, or targeting users - must clearly identify such information as being advertised or controlled, in an appropriate and transparent manner.
- (vi) **Identification of originator:** SSMLs must enable identification of the first originator of information, including SGI, in accordance with the procedure specified under Rule 4(2).
- (vii) **Proactive detection obligations:** SSMLs must endeavor to deploy technological measures to proactively identify rape and child sexual abuse material, or content previously taken down, including SGI, and to notify users upon such identification.

The Draft Amendments are an important step in recognising the risks posed by synthetic content. However, effective safeguards will require not only regulatory clarity and enforceable standards, but also close collaboration between stakeholders to ensure that safety measures keep pace with innovation.

MeitY invites feedback on the Draft Amendments till November 6, 2025.

