



# LEGISLATIVE UPDATE



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

### Background

On 10<sup>th</sup> February 2026, the Central Government, through the Union Ministry of Electronics and Information Technology (MeitY), notified an amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('IT Rules'). This amendment aims to address synthetic and AI-generated content (including deepfakes), adding new compliance duties for platforms and tightening timelines for takedown/handling of such content.

The amendment comes into effect on 20th February 2026.

### Salient Features

#### Key Definitions and Scope

The amendment introduces a formal definition for "*synthetically generated information*". The term refers to audio, visual, or audio-visual content that is artificially or algorithmically created, generated, modified, or altered using a computer resource. Such information is designed to appear real, authentic, or true, and to depict or portray any individual or event in a manner that is, or is likely to be, perceived as indistinguishable from a natural person or a real-world occurrence.

#### Exemptions

The amendment further clarifies that the following activities, when undertaken in good faith and without the intention of creating false or misleading records, shall not fall under the definition of "*synthetically generated information*":

- Routine editing, formatting, or technical correction of content.
- Transcription, translation, subtitling, dubbing, or the inclusion of accessibility features such as closed captions in existing content.

- Creation of documents, PDFs, research materials, training or educational content, or assistive media that do not purport to represent real individuals or actual events.

### Obligations of Intermediaries

**Periodic disclosures to users:** Intermediaries are required to inform users at least once every three months, in a simple and effective manner, through their terms of use, privacy policy, user agreement or similar instruments, and in English or any Eighth Schedule language that:

- Intermediaries are now also empowered to suspend user access in addition to terminating user access for violations of platform policies.
- Where non-compliance involves content that contravenes applicable law, the responsible user may be liable to penalties or punishment under the Information Technology Act, 2000 or other laws in force.
- Where violations amount to mandatorily reportable offences (including under the Bharatiya Nagarik Suraksha Sanhita, 2023 or the Prevention of Children from Sexual Offences Act, 2012 (POCSO Act), the intermediary will report such offences to the appropriate authorities.

### Additional disclosures for AI/synthetic content platforms:

Intermediaries providing computer resources to create or disseminate synthetically generated information must additionally inform users that:

- Unlawful use of AI tools may attract civil and criminal liability, including under laws such as the Bharatiya Nyaya Sanhita, 2023, POCSO Act, Representation of the People Act, Indecent Representation of Women Act, Sexual Harassment of Women at Workplace Act, and the Immoral Traffic (Prevention) Act.



# LEGISLATIVE UPDATE

- Consequences of non-compliance with may include:
  - Immediate removal or disabling of the offending content.
  - Suspension or termination of user accounts, without compromising evidentiary integrity.
  - Identification and disclosure of the violating user's identity to the complainant, where the complainant is a victim (or acting on behalf of a victim), in accordance with applicable law and
  - Mandatory reporting to law enforcement authorities where the conduct constitutes a reportable offence.

## **Duty to act on unlawful synthetically generated information:**

Where an intermediary becomes aware of either *suo motu*, upon actual knowledge, or through a grievance, complaint or information received under these IT Rules involving synthetically generated information, it must take expeditious and appropriate action. This represents a notable expansion from the previous iteration of the IT Rules. The amendment now introduces a *suo motu* obligation, meaning intermediaries are expected to proactively identify and address synthetically generated content even in the absence of an external complaint or notification.

Such action includes the measures specified, namely:

- Immediate removal or disabling of access to the offending content.
- Suspension or termination of the violating user account, without vitiating evidence.
- Identification and disclosure of the violating user's identity to a complainant who is a victim (or acting on behalf of a victim), in accordance with applicable law and
- Mandatory reporting to the appropriate authority where the conduct constitutes a reportable offence.

## **Mandatory deployment of preventive technical measures:**

Intermediaries must deploy reasonable and appropriate technical safeguards, including automated tools or equivalent mechanisms, to prevent users from creating or disseminating AI-generated content that violates applicable law. This includes proactive prevention of synthetically generated content that:

- Contains prohibited sexual or privacy-violative material, including: (i) child sexual exploitative or abuse material (CSEAM); (ii) non-consensual intimate imagery; (iii) obscene, pornographic, paedophilic, vulgar, indecent or sexually explicit content, or (iv) content invasive of bodily or personal privacy.
- Creates or alters false documents or electronic records.
- Facilitates explosives, arms or ammunition, including preparation, development or procurement.
- Falsely depicts or misrepresents a natural person or real-world event, in a manner likely to deceive, including

misrepresentation of identity, voice, conduct, actions or statements (i.e., deepfakes), whether the natural person is directly involved.

**Mandatory labelling and provenance for lawful AI-generated content:** For synthetically generated information not otherwise prohibited, intermediaries must ensure:

- Clear and prominent labelling, such that visual content carries a prominently visible disclosure, and audio content includes a prominently prefixed audio disclosure, enabling immediate identification that the content is AI-generated.
- Embedding permanent metadata or equivalent provenance mechanisms, to the extent technically feasible, including a unique identifier, and information identifying the intermediary's computer resource used to create, generate, modify or alter the content.

## **Obligations for Significant Social Media Intermediary (SSMI)**

**Mandatory user declaration prior to publication:** SSIMs that enable the display, upload, or publication of information must, before such content is made available, require users to declare whether the content is synthetically generated information. Subsequently, SSIMs must deploy appropriate technical measures, including automated tools or equivalent mechanisms, to verify the accuracy of user declarations, having regard to the nature, format, and source of the content. The responsibility extends beyond collection of declarations and includes reasonable and proportionate verification.

Where a user declaration or technical verification confirms that the content is synthetically generated, SSIMs must ensure that the content is clearly and prominently labelled, through an appropriate notice or disclosure, indicating that it is synthetically generated.

**Deemed failure of due diligence:** An SSMI will be deemed to have failed to exercise due diligence where it is established that the intermediary knowingly permitted or promoted, or failed to act upon, synthetically generated information in contravention of the IT Rules.

## **Faster takedown and compliance timelines**

The amendments introduce substantial tightening of enforcement and compliance timelines. These changes accelerate the response obligations of intermediaries in relation to unlawful content and user grievances.



# LEGISLATIVE UPDATE

Specifically, the amendment revises and replaces multiple timelines prescribed under Rule 3 of the IT Rules, thereby imposing stricter compliance requirements. Additionally, the amendments clarify that intermediaries must act promptly upon becoming aware of any violations involving synthetically generated information, whether through internal monitoring or upon receipt of a complaint.

The prescribed course of action may include, as appropriate, the disabling of access to the relevant content, suspension of user accounts, and reporting of the matter to competent authorities in accordance with applicable legal provisions.

Action	Older Timeline	New Timeline
Compliance with a Lawful Takedown Direction  [Rule 3(2)(b)]	36 hours	3 hours
Time period for disposal of grievances by a Grievance Redressal Office  [Rule 3(2)(a)]	15 days	7 days
Time period for an intermediary to address a complaint requiring urgent action.  [Rule 3(2)(a)]	72 hours	36 hours

Action	Older Timeline	New Timeline
Time period for removing content, pursuant to a complaint involving the sharing or dissemination of intimate images  [Rule 3(2)(d)]	24 hours	2 hours

## Analysis

The amendment places clear gatekeeping obligations on intermediaries for synthetically generated and AI-produced audio-visual content. Intermediaries are now required to deploy technical measures, including automated tools, to detect, prevent and verify unlawful synthetic content. Lawful synthetic content must be prominently labelled and embedded with tamper-resistant provenance metadata.

Statutory timelines for takedowns and notices are compressed to hours, which may be practically impossible to meet and will create significant operational burden. The amendment expressly empowers intermediaries to act *suo motu*, including suspending or terminating accounts and disabling access, a shift that appears to diverge from settled jurisprudence which recognized that social media intermediaries cannot be granted an adjudicatory role to determine legality of content. The amendment raises legal and operational risks that require careful mitigation and regulatory clarification.



# LEGISLATIVE UPDATE

## Annexure: Substitutions of Provisions

Rule	Old Provision	New Provision
Rule 3(2)(c)	(c) an intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be;	<p>(c) an intermediary shall periodically inform its users, at least once every three months, in a simple and effective manner through its rules and regulations, privacy policy, user agreement, or any other appropriate means, in English or any language specified in the Eighth Schedule to the Constitution, that -</p> <p>(i) in case of non-compliance with such rules and regulations, privacy policy or user agreement, by whatever name called, it has the right to terminate or suspend the access or usage rights of the users to the computer resource immediately, or to remove or disable access to non-compliant information, or both, as the case may be;</p> <p>(ii) where such non-compliance relates to the creation, generation, modification, alteration, hosting, displaying, uploading, publishing, transmitting, storing, updating, sharing or otherwise disseminating of information in contravention of any law for the time being in force, the user who is responsible for such noncompliance may be liable to penalty or punishment under the provisions of the Act or any other applicable law; and</p> <p>(iii) where such violation relates to the commission of an offence under any law for the time being in force, such as the Bharatiya Nagarik Suraksha Sanhita, 2023(46 of 2023) or the Protection of Children from Sexual Offences Act, 2012 (32 of 2012) which requires such offence to be mandatorily reported, reporting of such offence to the appropriate authority in accordance with the provisions of the applicable law;</p> <p>(ca) without prejudice to sub-clauses (i) and (ii) of clause (c), where an intermediary referred to under sub-rule (3) offers a computer resource which enables, permits or facilitates the creation, generation, modification, alteration, publication, transmission, sharing, or dissemination of information as synthetically generated information, such intermediary shall additionally inform its users that— (i) directing, instructing or otherwise causing the computer resource of the intermediary for creation, generation, modification, alteration publication, transmission, sharing, or dissemination of information as synthetically generated information in contravention of sub-clause (i) of clause (a) of subrule (3) may attract penalty or punishment as may be applicable under any law for the time being in force, including the provisions of the Act, the Bharatiya Nyaya Sanhita, 2023 (45 of 2023), the Protection of Children from Sexual Offences Act, 2012</p>



# LEGISLATIVE UPDATE

Rule	Old Provision	New Provision
		<p>(32 of 2012), the Representation of the People Act, 1951 (43 of 1951), the Indecent Representation of Women (Prohibition) Act, 1986(60 of 1986), the Sexual Harassment of Women at Workplace (Prevention, Prohibition And Redressal) Act, 2013 (14 of 2013), and the Immoral Traffic(Prevention) Act, 1956 (104 of 1956); and</p> <p>(ii) any such contravention of sub-clause (i) of clause (a) of sub-rule (3) may lead to— (I) the immediate disabling of access to or removal of such information; (II) suspension or termination of the user account of the user who violates this sub-rule without vitiating the evidence; (III) in accordance with applicable law, identification of such user and disclosure of the identity of the violating user to the complainant, where such complainant is a victim of, or an individual acting on behalf of a victim of, such contravention; and (IV) where such violation relates to the commission of an offence under any law for the time being in force, including the Bharatiya Nagarik Suraksha Sanhita, 2023 (46 of 2023) or the Protection of Children from Sexual Offences Act, 2012 (32 of 2012) which requires such offence to be mandatorily reported, reporting of such offence to the appropriate authority in accordance with the provisions of the applicable law;</p> <p>(cb) where an intermediary becomes aware, either on its own accord or upon receipt of actual knowledge or on the basis of any grievance, complaint or information received under these rules, of any violation of sub-rule (3), in relation to the creation, generation, modification, alteration, hosting, displaying, uploading, publishing, transmitting, storing, updating, sharing or otherwise dissemination of information as synthetically generated information covered under sub-clause (ii) of clause (a), it shall take expeditious and appropriate action, including those specified in sub-clause (ii) of clause (ca).</p>



# LEGISLATIVE UPDATE

Rule	Old Provision	New Provision
Rule 3(2)(d)	(d) an intermediary, on whose computer resource the information which is used to commit an unlawful act which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force is hosted, displayed, published, transmitted or stored shall, upon receiving the actual knowledge under clause (b) of sub-section (3) of Section 79 of the Act on such information, remove or disable access to such information within thirty-six hours of the receipt of such actual knowledge, and such actual knowledge shall arise only in the following manner, namely	(d) an intermediary, on whose computer resource the information which is used to commit an unlawful act which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force is hosted, displayed, published, transmitted or stored shall, upon receiving the actual knowledge under clause (b) of sub-section (3) of Section 79 of the Act on such information, remove or disable access to such information <u>within three hours</u> of the receipt of such actual knowledge, and such actual knowledge shall arise only in the following manner, namely
Rule 3(2)(d) (ii) (i)	<p>(i) issued by an officer authorised for the purpose of issuing such intimation by the Appropriate Government or its agency, being not below the rank of Joint Secretary or an officer equivalent in rank or where an officer at such rank is not appointed, a Director or an officer equivalent in rank, to the Government of India or to the State Government, as the case may be, and, where so authorised, acting through a single corresponding officer in its authorised agency, where such agency is so appointed:</p> <p>Provided that where such intimation is to be issued by the police administration, the authorised officer shall not be below the rank of Deputy Inspector General of Police, especially authorised by the Appropriate Government in this behalf:</p> <p>Provided further that all such intimations shall be subject to periodic review by an officer not below the rank of the Secretary of the concerned Appropriate Government once in every month to ensure that such intimations are necessary, proportionate, and consistent with clause (b) of sub-section (3) of Section 79 of the Act and this clause;</p>	<p><u>(i) issued by an officer authorised, by order in writing, for the purpose of issuing such intimation</u> by the Appropriate Government or its agency, being not below the rank of Joint Secretary or an officer equivalent in rank or where an officer at such rank is not appointed, a Director or an officer equivalent in rank, to the Government of India or to the State Government, as the case may be, and, where so authorised, acting through a single corresponding officer in its authorised agency, where such agency is so appointed:</p> <p><u>Provided that where such intimation is to be issued by the police administration, there may be one or more authorised officers, each not below the rank of Deputy Inspector General of Police, especially authorised by the Appropriate Government in this behalf:</u></p> <p>Provided further that all such intimations shall be subject to periodic review by an officer not below the rank of the Secretary of the concerned Appropriate Government once in every month to ensure that such intimations are necessary, proportionate, and consistent with clause (b) of sub-section (3) of Section 79 of the Act and this clause;</p>



# LEGISLATIVE UPDATE

Rule	Old Provision	New Provision
Rule 3(2)(a)	<p>Grievance redressal mechanism of intermediary: (a) The intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or [sub-rules (11) to (13) of Rule 4, or in respect of] any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall –</p> <p>[(i) acknowledge the complaint within twenty-four hours and resolve such complaint within a period of fifteen days from the date of its receipt:</p> <p>Provided that the complaint in the nature of request for removal of information or communication link relating to clause(b) of sub-rule (1) of Rule 3, except sub-clauses (i), (iv) and [(xi)], shall be acted upon as expeditiously as possible and shall be resolved within seventy-two hours of such reporting:</p> <p>Provided further that appropriate safeguards may be developed by the intermediary to avoid any misuse by users;](ii) receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.</p> <p>[Explanation.—In this rule, “prominently publish” shall mean publishing in a clearly visible manner on the home page of the website or the home screen of the mobile based application, or both, as the case may be, or on a web page or an app screen directly accessible from the home page or home screen.]</p>	<p>Grievance redressal mechanism of intermediary: (a) The intermediary shall prominently publish on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or [sub-rules (11) to (13) of Rule 4, or in respect of] any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall –</p> <p>[(i) acknowledge the complaint within twenty-four hours and resolve such complaint within a period of <u>seven days</u> from the date of its receipt:</p> <p>Provided that the complaint in the nature of request for removal of information or communication link relating to clause(b) of sub-rule (1) of Rule 3, except sub-clauses (i), (iv) and [(xi)], shall be acted upon as expeditiously as possible and shall be resolved within <u>thirty-six hours</u> of such reporting:</p> <p>Provided further that appropriate safeguards may be developed by the intermediary to avoid any misuse by users;](ii) receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.</p> <p>[Explanation. - In this rule, “prominently publish” shall mean publishing in a clearly visible manner on the home page of the website or the home screen of the mobile based application, or both, as the case may be, or on a web page or an app screen directly accessible from the home page or home screen.]</p>





# LEGISLATIVE UPDATE

Rule	Old Provision	New Provision
Rule 3(2)(b)	(b) The intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it:	(b) The intermediary shall, within <u>two hours</u> from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it:
Rule 4(4)	<p>A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of Rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:</p> <p>Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures:</p> <p>Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this subrule, including a periodic review of any automated tools deployed by such intermediary:</p> <p>Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.</p>	<p>A significant social media intermediary shall <u>deploy appropriate technical measures, including automated tools or other suitable mechanisms</u> to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of Rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule:</p> <p>Provided that the measures taken by the intermediary under this sub-rule shall be proportionate having regard to the interests of free speech and expression, privacy of users on the computer resource of such intermediary, including interests protected through the appropriate use of technical measures: Provided further that such intermediary shall implement mechanisms for appropriate human oversight of measures deployed under this subrule, including a periodic review of any automated tools deployed by such intermediary:</p> <p>Provided also that the review of automated tools under this sub-rule shall evaluate the automated tools having regard to the accuracy and fairness of such tools, the propensity of bias and discrimination in such tools and the impact on privacy and security of such tools.</p>





# LEGISLATIVE UPDATE

Rule	Old Provision	New Provision
Rule 7	Non-observance of Rules - Where an intermediary fails to observe these rules, the provisions of sub-section (1) of Section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.	Non-observance of Rules - Where an intermediary fails to observe these rules, the provisions of sub-section (1) of Section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and <u>the Bharatiya Nyaya Sanhita, 2023 (45 of 2023)</u> .

Please feel free to address any further questions or request for advice to:

**Dr. Shardul S. Shroff**

*Executive Chairman*

*shardul.shroff@AMSShardul.com*

**KS Roshan Menon**

*Principal Associate*

*roshan.menon@AMSShardul.com*

**Himali Sylvester**

*Associate*

*himali.sylvester@AMSShardul.com*

**Vishwajeet Deshmukh**

*Associate*

*vishwajeet.deshmukh@AMSShardul.com*

## Disclaimer

This is intended for general information purposes only. It is not a substitute for legal advice and is not the final opinion of the Firm. Readers should consult lawyers at the Firm for any specific legal or factual questions.