



Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes

प्रविष्टि तिथि: 06 AUG 2026 4:26PM by PIB Delhi

The Government remains conscious of the threats posed by deepfakes powered by Artificial Intelligence (AI), including synthetic audio, video and text. With an aim to ensure an open, safe, trusted and accountable cyberspace for users, Government of India has enacted the following laws and rules that address various aspects of the deepfake challenge:

The Information Technology Act, 2000 (“IT Act”)

- Section 43 prescribes penalty and compensation for damage to computers, computer systems etc.
- Section 66 prescribes punishment for computer related offences;
- Covers offences like identity theft (section 66C), impersonation (section 66D), privacy violations (section 66E), publishing or transmitting obscene or sexually explicit content (sections 67, 67A)
- Provision to issue blocking orders to intermediaries for blocking access to specific information/ link (section 69A)
- Provision to issue notice to intermediaries for removal of information being used to commit unlawful act (section 79)
- Besides, the Act also empowers Police to investigate offences (Section 78 and 80).

The Bharatiya Nyaya Sanhita, 2023 (“BNS”)

- Section 319 prescribes punishment for cheating by personation;
- Section 336 prescribes punishment for forgery (includes making false electronic records for the purpose of cheating or harming the reputation of any party).
- Section 353 aims to curb the spread of misinformation and disinformation by penalizing the act of making false or misleading statements, rumours, or reports that can cause public mischief or fear.
- Organised cybercrimes involving deepfake content can also be prosecuted under section 111.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules”)

The IT Rules cast specific obligations on intermediaries to observe due diligence while discharging their duties and shall inform the users of computer resources not to host, display, upload, modify, publish, transmit, update or share any information that :

- belongs to another person and to which the user does not have any right;
- obscene, pornographic, invasive of privacy, or promotes hate or violence;
- harms children;
- infringes any proprietary rights;
- misleads or deceives the addressee about the origin of message ;
- knowingly and intentionally communicates any misinformation; patently false and

untrue information or misleading information;

- impersonates others, including via AI;
- threatens national security or public order;
- violates any applicable law.

Intermediaries must clearly inform users through terms of service and user agreements about the consequences of sharing unlawful content, including content removal, account suspension, or termination.

Social media intermediaries having 50 lakhs or above registered user base in India (SSMIs) are required to comply with following additional obligations:

- SSMIs offering messaging services must help law enforcement trace originators of serious or sensitive content.
- To use automated tools to detect and limit spread of unlawful content.
- Publish compliance reports, appoint local officers, and share physical address based in India for compliances and law enforcement coordination.
- Offer voluntary user verification, internal appeals, and fair hearing before taking suo-moto action.

Grievance Redressal Mechanism:

Intermediaries are required to appoint Grievance Officers and resolve complaints within the prescribed timelines. Users can appeal online at <https://www.gac.gov.in> if their complaints are not addressed by the intermediaries' Grievance Officers. GACs ensure accountability and transparency of content moderation decisions.

The complaints registered with the Police are investigated by the concerned Law Enforcement Agencies (LEAs) under the relevant statutory framework. Since 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India, the States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cybercrime through their Law Enforcement Agencies (LEAs).

Recent Amendments:

On 10th February, 2026, the Government strengthened the regulatory framework by amending the IT Rules, 2021 to address harms arising from synthetically generated information (SGI), including deepfakes and AI-generated content.

Key points related to the amendment are as follows: -

- Intermediaries are required to ensure clear labelling and traceable metadata for permissible AI-generated content, so that users can easily identify synthetically generated material and prevent deception or misuse.
- It further strengthens user accountability and platform due diligence, including mandatory user awareness regarding legal consequences of unlawful AI-generated content and stronger compliance obligations for social media intermediaries.
- Importantly, the guidelines explicitly cover child sexual exploitation material, non-consensual intimate imagery, impersonation and other harmful AI-generated content, requiring platforms to prevent such content and take prompt action when detected.
- Strengthening of timelines for compliance, including reduced timelines for removal of unlawful information upon actual knowledge upon valid reasoned intimation from the Appropriate Government or court orders (timeline reduced from 36 hours to 3

hours) and for grievance redressal (including special categories such as nudity/impersonation etc.) (timeline reduced from 72 hours to 36 hours and 24 hours to 2 hours for sensitive matters, respectively).

- Intermediaries are obligated to deploy reasonable and appropriate technical measures, including automated tools or other suitable mechanisms, to not allow any user to create, generate, modify, alter, publish, transmit, share, or disseminate, as the case may be, any synthetically generated information that violates any law for the time being in force.
- IT Rules mandates the Significant Social Media Intermediaries (SSMIs) to take reasonable efforts to deploy appropriate technical measures, including automated tools or other suitable 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.

In case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, they lose their exemption from third party information provided under section 79 of the IT Act. They are liable for consequential action or prosecution as provided under any extant law.

AI Governance Guidelines:

The Government has adopted a balanced and pragmatic approach to AI governance. The **India AI Governance Guidelines**, released on **5 November 2025**, provide a risk-based and proportionate framework for the safe, trusted and responsible development and deployment of AI.

Strengthening capabilities under India AI Mission

The Safe & Trusted AI pillar of the IndiaAI Mission aims to promote the responsible development, deployment and adoption of AI through indigenous governance frameworks, standards, tools and evaluation mechanisms.¹³ Responsible AI projects have been approved in educational institutions across the country including deepfake detection.

Key initiatives related to deepfake detection include:

- Saakshya, multi-agent framework developed by IIT Jodhpur & IIT Madras for deep fake detection
- AI Vishleshak for improving Audio-Visual forgery detection system
- IIT Kharagpur's project on Real-Time Voice Deepfake Detection System _

Coordination Mechanism and Implementation Measures Adopted by Government

- GACs – Provide an appellate forum at the Central level to challenge decisions of intermediaries.
- Takedown Notices- Intermediaries, including social media intermediaries, are required to remove any unlawful information as and when brought to their knowledge either through a court order or through a reasoned intimation, in writing from the Appropriate Government or its agency. Such unlawful information includes information 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. The notices for takedown of any such

information on the intermediary platform are sent directly by the respective appropriate governments or their authorised agencies where the appropriate government can be both the State and Central Government as per the Seventh Schedule to the Constitution.

- Indian Cyber Crime Coordination Centre (I4C) – Coordinates actions related to cybercrimes across States. Empowers agencies to issue notices for removal or disabling access to unlawful content including deepfakes under the IT Act read with IT Rules, 2021.
- SAHYOG Portal (managed by I4C) – Enables automated, centralized removal notices to intermediaries. Appropriate Government and its authorised agencies across India use it to request removal of unlawful content.
- National Cyber Crime Reporting Portal – Citizens can report incidents through this portal at <https://cybercrime.gov.in> which has special focus on cyber crimes against women and children. Deepfakes, financial frauds, and content misuse are all reportable. A helpline number 1930 is also functional.
- Police – Police officers investigate cyber crimes.
- Samanvaya Platform: The Samanvaya Platform strengthens cyber fraud investigations by providing analytics-based interstate linkages of criminals and crimes. Its ‘Pratibimb’ module maps locations of criminals and crime infrastructure, giving officers actionable visibility. So far, it has led to the arrest of **12,987 accused, 1,51,984 criminal linkages, and 70,584 cyber investigation** assistance requests, helping dismantle organised cyber fraud networks efficiently.

Advisories and Standard Operating Procedure (SOP):

The government has issued multiple advisories to the intermediaries, including the Social Media Intermediaries, emphasizing the observance of due diligence obligations under the IT Act and IT Rules. The details of the advisories issued and SOPs formulated are as follows:

- An advisory dated 09.02.2026 was issued to intermediaries regarding the responsible handling of information relating to religious matters.
- An advisory dated 16.03.2026 was issued to intermediaries with respect to the generation, hosting, publication, transmission, sharing or uploading of abusive, defamatory, objectionable, derogatory and misleading synthetically generated information.
- A Standard Operating Procedure (“SoP”) to curtail dissemination of Non-Consensual Intimate Imagery (NCII) content on online platforms has been formulated and released on 11.11.2025. The SoP provides detailed guidance for victims, intermediaries and law enforcement agencies to ensure prompt and uniform action against the online dissemination of NCII content including intimate or morphed images shared without consent.

Awareness campaigns

MeitY observes the Cyber Security Awareness Month (NCSAM) during October of every year, Safer Internet Day on 2nd Tuesday of February every year, Swachhta Pakhwada from 1st to 15th February of every year and Cyber Jagrookta Diwas (CJD) on 1st Wednesday of every month by organising various events and activities for citizens as well as the technical cyber community in India.

CERT-In:

The Indian Computer Emergency Response Team also regularly issues guidelines on AI-related threats and countermeasures, including deepfake; shares safety and security tips and awareness posters, infographics and videos on its official websites and social media handles and is aimed at sensitizing internet

users on cyber security attacks and frauds including online safety measures for children. It has published an advisory in November 2024 on deepfake threats and measures that need to be followed to stay protected against deepfakes.

This information was submitted by Union Minister of State for Electronics and Information Technology Shri Jitin Prasada in Lok Sabha on 05.08.2026.

Vinod Kumar / Kanishk Sharma

(रिलीज़ आईडी: 2295500) आगंतुक पटल : 2945
इस विज्ञप्ति को इन भाषाओं में पढ़ें: Urdu , हिन्दी , Tamil