GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2302
TO BE ANSWERED ON: 08.08.2025

REGULATORY FRAMEWORKS TO IDENTIFY AND COMBAT DEEPFAKES

2302. SHRI KARTIKEYA SHARMA:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the mechanisms and regulatory frameworks currently in place to identify and combat deepfakes and related synthetic media frauds, the details thereof;
(b) the total number of cases of deepfake and synthetic media fraud reported till date, along with action taken, such as takedowns, investigations, prosecutions, the details thereof, State-wise; and
(c) whether any indigenous technology or platform is being developed or proposed to detect and mitigate such threats, including grants, Research and Development (R&D) collaboration, or pilot deployments with Startups or research institutions?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (c): Government remains conscious of the threats posed by deepfakes powered by Artificial Intelligence (AI), including synthetic audio, video and text. Such content can seriously impact a person's dignity, reputation, and right to privacy. It also raises concerns about platform accountability.

With an aim to ensure an open, safe, trusted and accountable cyberspace for users, Government of India has enacted the following laws that address various aspects of the deepfake challenge:

The Information Technology Act, 2000 ("IT Act")

- 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)
- Provisions to issue notice to intermediaries for removal of information being used to commit unlawful act (section 79)

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021") – Ensuring Platform Accountability:

- Ministry of Electronics and Information Technology ("MeitY"), after extensive consultations with relevant stakeholders, notified the IT Rules, 2021 (amended in 2022 and 2023) to address emerging harms from misuse of technologies, including AI.
- The Rules mandate intermediaries to exercise due diligence and prevent hosting or transmission of unlawful content by themselves or their users.

Digital Personal Data Protection Act, 2023 ("DPDP Act")– Ensures that personal data is processed lawfully by the Data Fiduciaries (including AI companies) with user consent and reasonable security safeguards. Deepfakes using personal data without consent can attract penalties under this Act.

Bharatiya Nyaya Sanhita, 2023 ("BNS")– 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.

These Acts and Rule-making thereunder, as applicable, remains technology-neutral – as the provisions are applicable irrespective of whether the content is AI-generated or not. So, AI-based harms are also actionable under current laws.

Government actively engages with stakeholders and social media platforms to ensure strict implementation of existing laws, including in cases involving AI-generated harms.

- In this direction, Advisories dated 26.12.2023 and 15.03.2024 were issued through which intermediaries were reminded about their due-diligence obligations outlined under IT Rules, 2021 and advised on countering unlawful content including malicious 'synthetic media' and 'deepfakes'.

These advisories include *inter-alia* the following directions that—

- Intermediaries should identify and remove misinformation or information that impersonates another person, including those created using deepfakes.
- Users must also be made aware that such content may be inaccurate or misleading.
- Intermediaries must comply with the orders of the Grievance Appellate Committee within the timeline mentioned in the order and publish a report.
- Unreliable or under-tested AI models or algorithms, etc. should be available for use in India only after appropriately labelling the possible inherent unreliability of the output and users must be explicitly informed about such unreliability.

Key provisions under IT Rules, 2021:

Provision	**Details**

Restricted information under Rule 3(1)(b)	Restricts information/content that, among other things, • is obscene, pornographic, invasive of privacy, or promotes hate or violence; • harms children; • misleads or deceives, including through deepfakes; • impersonates others, including via AI; • threatens national security or public order; • violates any applicable law.
User Awareness Obligations	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.
Accountability in Content Removal	Intermediaries must act expeditiously to remove unlawful content upon court orders, government notice, or user grievances, within prescribed timelines.
Grievance Redressal	• Intermediaries to appoint Grievance Officers • Mandates to resolve complaints through removal of unlawful content within 72 hours. • Content violating privacy, impersonating individuals, or showing nudity must be removed within 24 hours against any such complaint.
Grievance Appellate Committees (GACs) Mechanism	Users can appeal online at www.gac.gov.in if their complaints are not addressed by the intermediaries' Grievance Officers. GACs ensure accountability and transparency of content moderation decisions.
Additional Obligations of significant social media intermediaries (SSMIs) (i.e., social media intermediaries having 50 lakhs or above registered user base in India)	• SSMIs offering messaging services must help law enforcement trace originators of serious or sensitive content. • SSMIs to use automated tools to detect and limit spread of unlawful content. • SSMIs to publish compliance reports, appoint local officers, and share physical address based in India for compliances and law enforcement coordination. • SSMIs to offer voluntary user verification, internal appeals, and fair hearing before taking suo-moto action.

India's multi-layered cyber response ecosystem includes institutional, regulatory, reporting, and public awareness mechanisms to address cyber crimes, user grievances, and unlawful content, including deepfakes:

- **GACs** – Provide an appellate forum at the Central level to challenge decisions of intermediaries.

- **Indian Cyber Crime Coordination Centre (I4C)** – Coordinates actions related to cyber crimes 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. All 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.
- **CERT-In** – The Indian Computer Emergency Response Team (CERT-In) regularly issues guidelines on AI-related threats and countermeasures, including deepfake. CERT-In has published an advisory in November 2024 on deepfake threats and measures that need to be followed to stay protected against deepfakes.
- **Police** – Police officers investigate the cyber crimes.
- **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.

India's cyber legal framework, backed by the IT Act, BNS, and institutions like GAC, CERT-In, and I4C, is well-equipped to tackle evolving online harms and cyber crimes.

******