GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 4523**
TO BE ANSWERED ON: 20.08.2025

**COORDINATION BETWEEN LAW ENFORCEMENT AGENCIES AND SOCIAL MEDIA INTERMEDIARIES**

**4523. SHRI RAMASAHAYAM RAGHURAM REDDY:**
**SHRI BRIJENDRA SINGH OLA:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether the Government is aware of the growing misuse of social media platforms such as Facebook, Instagram, X (formerly Twitter) and YouTube for online abuse including threats, character assassination, fake news, hate speech and harassment particularly targeting women, children, public figures and activists;
(b) the status of fake news and hate speech on social media platforms across the country;
(c) whether complaints have been received where such platforms failed to act swiftly in removing offensive content or tracing offenders despite repeated requests by victims and if so, the details thereof;
(d) whether a formal coordination mechanism exists between law enforcement agencies and social media intermediaries to ensure timely takedown of abusive content and identification of offenders;
(e) whether there is any independent body to keep check in this regard, if so, the details thereof and if not, the reasons therefor; and
(f) the details of concrete steps taken by the Government to check fake or hate speech being circulated on social media platforms?

**ANSWER**

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

(a) to (f): Government remains conscious of the risks and harms arising from the misuse of digital technologies including the misuse of social media platforms for online abuse/harassment, spreading fake news and hate speech.

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 unlawful content and platform accountability on social media:

- **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, 67B), and provisions 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). Empowers Police to investigate offences (section 78), enter public place and search and arrest suspected person (section 80).

- **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.
    - Part-III of the Rules inter alia provides for Code of Ethics to be followed by publishers of news & current affairs. It includes adherence to the Programme Code laid down under the Cable Television Networks Act, 1995, and the Norms of Journalistic Conduct under the Press Council Act, 1978.A three-tier grievance redressal mechanism for users of news and current affairs content is also provided.
- **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.
- **Protection of Children from Sexual Offences (POCSO) Act, 2012–** To safeguard children against sexual abuse and sexual harassment:
    - Section 13 criminalises the use of a child in any form of media—whether electronic, printed, or broadcast—for the purpose of sexual gratification. This includes:
        - Representation of the sexual organs of a child,
        - Use of a child in real or simulated sexual acts (with or without penetration),
        - Indecent or obscene representation of a child.
    - Section 14 prescribes punishment of imprisonment for not less than five years and a fine for the first offence. For subsequent convictions, the punishment increases to imprisonment for not less than seven years and a fine. Section 15 lays out a graded punishment system for possessing, storing, or failing to report pornographic material involving children.
- **Bharatiya Nyaya Sanhita, 2023 ("BNS")**–
    - Provides punishment for offences like voyeurism (Section 77), stalking (Section 78), insulting the modesty of woman (Section 79), obscene acts and songs (Section 296), sale of obscene material including display of any such content in electronic form (Section 294)
    - Also covers offences like deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs, bywords, either spoken or written, or by signs or by visible representations or through electronic means(Section 299) and cheating by personation (Section 319). Further, 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 can also be prosecuted under section 111.

- **Indecent Representation of Women (Prohibition Act), 1986**– Section 4 provides for punishment for indecent representation of women through advertisements or in publications, writings, paintings, figures, or in any other manner.

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 hosting, storing, transmitting, displaying or publishing information/content that, among other things, is:<br>• obscene, pornographic, invasive of another's privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, or promoting hate or violence;<br>• harmful to child;<br>• deceives or misleads, including through deepfakes;<br>• impersonates others, including via AI;<br>• threatens national security or public order;<br>• 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<br>• Mandates to resolve complaints through removal of unlawful content within 72 hours.<br>• 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 atwww.gac.gov.in if their complaints are not addressed by the intermediaries' Grievance Officers. GACs ensure accountability and transparency of content moderation decisions. |
| **Assistance by Intermediaries to Government Agencies** | Intermediaries mustprovide information under their control or assistance to authorised Government agencies for identity verification, or for the prevention, detection, investigation, or prosecution of offences, including cyber security incidents. |
| **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.<br>• SSMIs to use automated tools to detect and limit spread of unlawful content.<br>• SSMIs to publish compliance reports, appoint local officers, and share physical address based in India for compliances and law enforcement coordination.<br>• 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:

- **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. An empowered 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 athttps://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, SwachhtaPakhwada 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, POCSO Act, BNS and institutions like GAC, CERT-In, and I4C, is well-equipped to tackle evolving online harms and cyber crimes.

******