

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3971
TO BE ANSWERED ON: 12.08.2026

FAKE CONTENT ON SOCIAL MEDIA PLATFORMS

†3971. DR. ANAND KUMAR:

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

- (a) whether fake, misleading and manipulated content is being rapidly generated and disseminated on WhatsApp, Telegram and other social media platforms and if so, the details thereof;
- (b) whether the Government has reviewed the effectiveness of existing legal provisions against those who create and deliberately propagate such content and if so, the details thereof;
- (c) whether the Government proposes to introduce a new mechanism or legal provision to ensure the identification of culprits in such cases and punitive and criminal action against them instead of being limited merely to the removal of such content; and
- (d) the details of steps being taken by the Government to effectively curb the creation and dissemination of fake content and to enhance the accountability of social media platforms?

ANSWER

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

(a) to (d): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. The existing legal framework including The Information Technology Act, 2000 (“IT Act”) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules”), together, have put in place a framework to deal with fake, misleading and manipulated content in the digital space and impose clear obligations on intermediaries to ensure accountability.

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

- Provision to issue blocking orders to intermediaries for blocking access to specific information/link (section 69A).
- Provision to issue notice to intermediaries for removal or disabling access of information being used to commit unlawful acts (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 misleads or deceives, including through deep-fakes, impersonates others including via AI, threatens national security or public order or 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 addresses 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.

Recent Amendments:

On 10th February, 2026, the Government strengthened the regulatory framework by amending the IT Rules 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.

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.

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 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.

PIB Fact Check Unit

The Press Information Bureau (“PIB”) has been at the forefront of taking proactive measures to combat fake news related to the Government of India. In November 2019, PIB established a Fact Check Unit with the purpose of tackling the issue of fake news pertaining to the Government of India, its various ministries, Departments, Public Sector Undertakings, and other Central Government organizations.

The unit verifies claims about government policies, regulations, announcements and measures. Through an established rigorous fact-checking procedure, the PIB Fact Check Unit helps in dispelling myths, rumours and false claims, and provides accurate and reliable information to the public.

‘Police’ and ‘Public Order’

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).
