

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3970
TO BE ANSWERED ON: 12.08.2026

REGULATION AND MISUSE OF ARTIFICIAL INTELLIGENCE

3970. DR. MOHAMMAD JAWED:

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

- (a) whether the Government has enacted or proposes to enact a legal framework regulating the development and use of Artificial Intelligence (AI) in the country and if so, the details thereof;
- (b) whether the Government is aware of the misuse of AI on social media for fraud, impersonation, deepfakes, misinformation and other unlawful activities;
- (c) if so, the details of such cases reported during each of the last five years along with the action taken thereon; and
- (d) whether any mechanism is put in place to monitor AI-enabled misuse on social media platforms and coordinate with intermediaries and law enforcement agencies for its detection and prevention and if so, the details thereof?

ANSWER

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

(a) to (d): India's Artificial Intelligence (AI) policy is based on Prime Minister Narendra Modi's vision of democratizing technology. It is aimed at creating economic opportunities and employment for youth, while addressing risks associated with AI.

India's AI strategy builds on India's vibrant IT sector with annual revenue of 300 billion dollars and 60 lakh strong workforce. The IndiaAI Mission has seven pillars including development of AI models, applications, datasets, talent development and affordable compute.

India AI Governance Guidelines were released on 5th November 2025, providing a comprehensive national framework for the safe, responsible and inclusive development and deployment of Artificial Intelligence in the country.

Pursuant to the Guidelines, the following institutional mechanisms have been initiated:

- AI Governance and Economic Group (AIGEG), a high-level inter-ministerial body to steer the development of India's national AI governance strategy;
- Technology and Policy Expert Committee (TPEC), to support technical and policy recommendations; and
- AI Safety Institute (AISI), to undertake safety research, develop standards, test AI systems and evaluate emerging risks.

To help achieve the aim at ensuring an Open, Safe and Trusted and Accountable Internet for all users, the Government adopts a consultative approach in matters relating to the legal and regulatory framework governing the digital ecosystem and regularly engages with relevant stakeholders to examine the legal, policy and institutional framework relating to emerging issues in the cyberspace, in light of technological developments and public interest.

Any legislative or regulatory measures, if considered necessary, are processed in accordance with the extant policy and established legislative procedures of the Government.

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 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.

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 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.

‘Police’ and ‘Public Order’ are State subjects under the Seventh Schedule to the Constitution of India. Accordingly, the States and Union Territories (UTs) are primarily responsible for the prevention, detection, investigation, and prosecution of cybercrime. The Central Government, through the Ministry of Home Affairs (MHA), supplements the efforts of States and UTs by providing policy guidance, technological support, capacity-building assistance, and financial resources to strengthen cybercrime management and enforcement capabilities. The Ministry of Home Affairs has set up the ‘Indian Cyber Crime Coordination Centre’ (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.

The ‘National Cyber Crime Reporting Portal’ (NCRP) (<https://cybercrime.gov.in>) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law. A toll-free Helpline number ‘1930’ has been operationalized to get assistance in lodging online cyber complaints.

The ‘Citizen Financial Cyber Fraud Reporting and Management System’ (CFCFRMS), under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters
