

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3898
TO BE ANSWERED ON: 04.04.2025

LEGISLATION TO TACKLE DEEPFAKE VIDEOS

3898. DR.M. THAMBIDURAI:

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

- (a) whether it is a fact that deepfake videos are increasing day by day;
- (b) if so, the details thereof;
- (c) whether Government has any plans to bring a new legislation to tackle the menace of deep fake videos;
- (d) if so, the details thereof and if not, whether the existing provisions of the Act and Rules are capable to take care of these issues; and
- (e) the steps taken by Government to tackle the situation?

ANSWER

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

(a) to (e): The policies of Government of India are aimed at ensuring a safe, trusted and accountable cyberspace for users in the country. Key regulatory initiatives taken by the Central Government to address issues of misinformation and deepfakes, are as under:

- The Information Technology Act, 2000 (“IT Act”) and the rules made there under have created a legal framework designed to protect the internet from unlawful activities to ensure safety and trust among the users.
- The IT Act provides for punishment for various offences considered as cybercrimes such as identity theft, cheating by personation, violation of privacy, publishing/transmitting material that is obscene/ containing sexually explicit act, etc., depicting children in sexually explicit act/transmitting/ browsing child sexual abuse material, etc.
- The IT Act and the rules made apply to any information that is generated using Artificial Intelligence (“AI”) tools or any other technology and those which are generated by users themselves for the purpose of defining offences.
- To protect users in India and the Indian internet at large from the emerging harms emanating from the misuse of technologies including AI and to ensure accountability towards law of the land, the Ministry of Electronics and Information Technology (“MeitY”) regularly engages with and receives inputs from the industry for promoting ethical use of technologies.

- Accordingly, the Central Government after extensive consultations with relevant stakeholders notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules, 2021”) and its subsequent amendments under the IT Act to address various emerging issues on the cyberspace.
- The IT Rules, 2021 casts specific obligations on intermediaries, including social media intermediaries to not host, store or publish any information violative of any law.
- They are also obligated to ensure their accountability that includes their expeditious action towards removal of the unlawful information categorised under the IT Rules, 2021 as notified by the appropriate government’s or on the basis of grievances received against any unlawful information.
- Such unlawful information comprises any information that, among other things, is harmful to child or that is promoting enmity between different groups on the grounds of religion or caste with the intent to incite violence, or that deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature, or that threatens the unity, integrity, defence, security or sovereignty of India, public order, or that violates any law for the time being in force.
- Where any information is categorised as unlawful under the IT Rules, 2021, any user may make a request to the Grievance Officer of the concerned intermediary on whose platform such unlawful information is made available to the public. Upon receipt of such request, the intermediary is required to act expeditiously within the timelines prescribed under IT Rules, 2021.
- Also, under the IT Rules, 2021, the Government has established Grievance Appellate Committees to allow users and victims to appeal online on www.gac.gov.in against decisions taken by the Grievance Officers of intermediaries in case they are dissatisfied with the decision of the Grievance Officer.
- Taking into cognizance that there is an urgent need to address the harms and criminalities being committed through widespread circulation of misinformation and deepfakes powered by AI, MeitY conducted multiple consultations with industry stakeholders/ social media platforms to discuss the challenges identified in combating deepfakes and has issued advisories time to time, through which the intermediaries were reminded about compliance with their due-diligence obligations outlined under the IT Rules, 2021 and advised on countering unlawful content including malicious “synthetic media” and “deepfakes” to curb deepfakes and promptly remove harmful content online.
- The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis. In this context, an advisory on safety measures to be taken to minimize the adversarial

threats arising from Artificial Intelligence (AI) based applications was published in May 2023. CERT-In has published an advisory in November 2024 on deepfake threats and measures that need to be followed to stay protected against deepfakes.

- CERT-In has taken following measures to enhance awareness among users and organisations for safe usage of digital technologies and tackling digital risks:
 - CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities including social engineering, phishing and vishing campaigns and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.
 - CERT-In has issued an advisory to various Ministries in November 2023 outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.
 - CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.
 - CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.
 - Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.
 - CERT-In is regularly carrying out various activities for awareness and citizen sensitization with respect to cyber-attacks and cyber frauds. CERT-In is observing the Cyber Security Awareness Month (NCSAM) during October of every year, Safer Internet Day on 1st Week Tuesday of February Month every year, SwachhtaPakhwada from 1 to 15 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 conducted several awareness activities such as Quiz, webinars, Capture the Flag event in collaboration with Government and industry partners during NCSAM 2024 with the theme “SatarkNagrik, Secure our World”.
- In addition, the Ministry of Home Affairs (“MHA”) has established the Indian Cyber Crime Coordination Centre (“I4C”) to provide a framework and eco-system for LEAs to deal with cyber-crimes in a comprehensive and coordinated manner. MHA has also launched the National Cyber Crime Reporting Portal (<https://cybercrime.gov.in>) to enable the public to report all types of cyber-crimes including cyber financial frauds.
- Cybercrime incidents reported on this portal are routed to the respective State/UT law enforcement agency for further handling as per the provisions of law. The portal has distinct mechanisms for registering complaints related to financial frauds. A toll-free Helpline number ‘1930’ has been operationalised to get assistance in lodging online complaints.
