GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2995
TO BE ANSWERED ON 11.03.2026

ONLINE HARASSMENT OF WOMEN

2995. SHRI DEEPENDER SINGH HOODA:

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

(a) whether the Government has any data on cases of cyberbullying, online harassment, deepfake misuse and other technology-enabled offences targeting women during the last five years;
(b) if so, the details of reported cases and convictions, State-wise including Haryana;
(c) whether the Government has issued any specific guidelines/standard operating procedures for preventing the creation and circulation of deepfake content targeting women;
(d) the details of the measures taken/being taken to strengthen the capacity of law-enforcement agencies, including cyber-forensics infrastructure to investigate such crimes quickly and effectively; and
(e) whether the Government proposes to launch a national programme for safety of women on digital platforms including awareness campaigns for teenagers and young users and if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATIONTECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (e): The policies of Government of India are aimed at ensuring open, safe, trusted and accountable cyberspace for users in the country. The Government is also cognizant of the risks and harms arising from the misuse of digital technologies including deepfakes.

Legal safeguards in place are as follows;

Information Technology (IT) Act, 2000
IT Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021) deal with unlawful and harmful content in the digital space and impose clear obligations on intermediaries to ensure accountability.

The IT Act penalises publishing or transmission of material containing sexually explicit act in electronic form (section 67A and 67B) and publishing or transmitting of obscene material in electronic form (section 67). These are punishable with imprisonment for a period that may extend to three and five years respectively.

In addition, following relevant sections of The Bharatiya Nyaya Sanhita, 2023 (‘BNS 2023’) are also applicable:

- Section 294 deals with offences related to sale of obscene material including display of any such content in electronic form.
- Section 296 provides punishment for offences like obscene acts and songs.
- 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.

The IT Rules cast specific legal obligations on intermediaries, including the social media intermediaries to make reasonable efforts to ensure that users of their computer resources do not host, display, upload, modify, publish, transmit, store, update or share any information that is obscene, pornographic, paedophilic, harmful to child, invasive of privacy, insulting or harassing on the basis of gender or violates any law for the time being in force.

The rules also mandate the expeditious removal of such unlawful content within the stipulated timelines.

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 and large social media platforms to deploy reasonable technical measures to prevent the creation and dissemination of unlawful AI-generated content, including content that is obscene, misleading, impersonating individuals, or harmful to children
- Platforms are also 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 large social media intermediaries
- Importantly, the regulatory framework explicitly covers 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
- 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 such synthetically generated information that violates any law for the time being in force, including Bharatiya Nyaya Sanhita, 2023 and Protection of Children from Sexual Offences Act, 2012
- Social media platforms and other intermediaries are required to remove unlawful content within three hours of the receipt of an order of a court of competent jurisdiction or a reasoned intimation by the Appropriate Government or its agency

Further, 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.

CERT-In regularly shares safety and security tips and awareness posters, info-graphics and videos on its official websites and social media handles and is aimed at sensitizing internet users on cyber security attacks and frauds including online safety measures for children.

The IT Act has enabling provisions for Central Government to notify any department, body or agency of the Central Government or a State Government as an "Examiner of Electronic Evidence" (Section 79A of IT Act) and to issue certificates for the verification of electronic records and ensuring their admissibility in judicial proceedings.

Ministry of Electronics & IT is implementing a project on 'Information Security Education and Awareness (ISEA) for generating human resources in Information Security and creating general awareness on various aspects of cyber hygiene & cyber security among the masses. So far, 4,309 awareness workshops conducted across the country covering over 9.63 lakh participants, including school/colleges students, teachers, law enforcement, government personnel, and general public. Around 15 crores estimated beneficiaries covered through indirect mode.

National Institute of Electronics and Information Technology (NIELIT) provides digital literacy courses such as Awareness in Computer Concept (ACC), Course on Computer Concepts (CCC) etc. NIELIT has trained 43 lakh+ candidates under various courses, including digital literacy and cyber security awareness and training is delivered through a wide network of 56 NIELIT Centers and 8500+ Accredited Training Partners/Facilitation Centers.

'Police' and 'Public Order' are State subjects as per the Constitution of India and States are primarily responsible for prevention, detection and investigation through their law enforcement machinery. The Law Enforcement Agencies take legal action against the cyber-crime offenders as per the provisions of applicable laws.

The National Cyber Crime Reporting Portal ("NCRP") (https://cybercrime.gov.in) has been launched, as a part of the Indian Cyber Crime Coordination Centre("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.

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The details can be accessed in their website https://ncrb.gov.in.

******