GOVERNMENT OF INDIA
MINISTRY OF WOMEN AND CHILD DEVELOPMENT

RAJYA SABHA
UNSTARRED QUESTION NO. 1431
TO BE ANSWERED ON 11.02.2026

MISUSE OF FAKE PROFILES OF WOMEN

1431. SHRI KARTIKEYA SHARMA:

Will the Minister of Women and Child Development be pleased to state:

(a) whether the Ministry has taken cognisance of the increasing misuse of fake profiles and impersonation of women on social media and dating platforms;

(b) the specific interventions being undertaken under Mission Shakti to address online gender-based violence, including deepfakes and non-consensual sharing of images;

(c) whether Government is considering the formulation of a digital rights or safety framework to safeguard the dignity, privacy and security of women online; and

(d) the details of awareness and outreach programmes being conducted to educate young women on digital privacy, reporting mechanisms and legal remedies against cyber harassment?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF WOMEN AND CHILD DEVELOPMENT
(SHRIMATI SAVITRI THAKUR)

(a) to (d): "Police" and "Public Order" are State subjects under the Seventh Schedule of the Constitution of India. Accordingly, States and Union Territories (UTs) are primarily responsible for the prevention, detection, investigation and prosecution of crimes, including cyber crimes, through their respective Law Enforcement Agencies (LEAs). The Central Government supplements State/UT efforts through policy interventions, advisories, coordination mechanisms, legal frameworks and financial assistance for capacity building.

The Government has taken cognisance of the increasing misuse of digital platforms, including social media and dating applications, through fake profiles, impersonation of women, cyber harassment, deepfakes and non-consensual sharing of images. While digital technologies offer significant opportunities for women in education, employment, access to information and

public service delivery, the Government also recognises that misuse of emerging technologies poses serious risks to the dignity, privacy, safety and well-being of women and children.

The Ministry of Women and Child Development works in close coordination with the Ministry of Home Affairs and the Ministry of Electronics and Information Technology to address online gender-based violence, including impersonation, misuse of fake profiles, circulation of obscene content, non-consensual intimate imagery (NCII) and deepfakes, through inter-ministerial consultations, advisories, regulatory measures and victim-support mechanisms. Under Mission Shakti, a holistic and victim-centric approach is adopted to strengthen safety, security and empowerment of women, including protection against technology-facilitated crimes. Women affected by cyber harassment or online abuse are provided access to integrated services including legal assistance, counselling and facilitation for reporting offences through One Stop Centres established across the country. Under the Nirbhaya Fund, Government has implemented a scheme of Cyber Crime Prevention against Women and Children (CCPWC). A cybercrime reporting portal www.cybercrime.gov.in has been put in place. Further, a cybercrime helpline 1930 is also functional. Further, the Ministry of Home Affairs through social media and other media channels continuously raises awareness about various forms of cyber-crimes and the available redressal mechanisms including reporting.

The Information Technology Act, 2000 provides a comprehensive statutory framework to address cyber offences. Section 43 read with Section 66 provides punishment for unauthorised access and computer-related offences; Section 66C for identity theft; Section 66D for cheating by personation using computer resources, including creation and use of fake profiles; Section 66E for violation of privacy, including non-consensual intimate imagery; Sections 67, 67A and 67B for publishing or transmitting obscene, sexually explicit and child sexual exploitative and abuse material; and Section 69A for blocking of unlawful content. Sections 78 and 80 empower law enforcement agencies to investigate cyber offences and conduct search and arrest. The Act is technology-neutral and applies uniformly to all computer resources, including those using artificial intelligence or other emerging technologies, without distinction between user-generated and machine-generated content.

Further, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2022, 2023 and 2025, mandate intermediaries to

observe due diligence under Section 79 of the IT Act. Rule 3(1)(b) prohibits hosting or transmission of unlawful content, including impersonation, violation of privacy, obscene or sexually explicit material, content insulting or harassing on the basis of gender and content harmful to children. Rule 3(2)(b) provides clear victim centric protocol for reporting and mandates removal or disablement of access to content depicting nudity, impersonation or NCII within twenty-four hours of complaint. The Rules require appointment of Grievance Officers, time-bound grievance redressal, periodic user awareness and provide an appellate mechanism through Grievance Appellate Committees (GACs). Failure to comply results in loss of safe harbour protection under Section 79 of the IT Act and attracts legal action.

Recognising the growing misuse of generative artificial intelligence tools and synthetically generated information, including deepfakes, the Ministry of Electronics and Information Technology has prepared amendments to the IT Rules, 2021 to further strengthen intermediary due diligence.

In October 2025, the Ministry of Electronics and Information Technology issued a Standard Operating Procedure under Rule 3(2)(b) of the IT Rules, 2021 to curtail dissemination of NCII content. The SOP provides a victim-centric protocol with multiple reporting channels including One Stop Centres, intermediary grievance mechanisms, the National Cyber Crime Reporting Portal and law enforcement agencies; mandates removal or disablement of such content within twenty-four hours; requires deployment of crawler-based and hash-matching technologies to prevent re-upload or resurfacing; and provides for coordinated action including de-indexing by search engines and cooperation with the Indian Cyber Crime Coordination Centre.

The Government has also issued advisories to intermediaries during 2023–2025 reiterating statutory obligations under the IT Act, 2000 and the IT Rules, 2021 to prevent hosting, publication or dissemination of impersonation, deepfakes, NCII and other unlawful content. These advisories emphasise strict adherence to due diligence requirements, expeditious compliance with court orders and lawful government directions, deployment of proactive technology-based measures and awareness of penal consequences under the IT Act, the Bharatiya Nyaya Sanhita, 2023 and other applicable laws.

Further, the Digital Personal Data Protection Act, 2023 establishes a comprehensive, rights-based and technology-neutral framework governing processing of digital personal data. The Act mandates lawful and consent-based data processing, robust security safeguards, breach notification, accountability of data fiduciaries and processors, enhanced obligations for significant data fiduciaries and special protections for children through verifiable parental consent. It also provides individuals with enforceable rights including access, correction, erasure and grievance redressal, thereby strengthening privacy protection and complementing the IT Act in addressing misuse of personal data and impersonation of women online.

In addition, sustained awareness and outreach programmes are undertaken through Mission Shakti, One Stop Centres, digital campaigns, workshops and coordination with States and UTs to educate women and girls on safe and responsible use of digital platforms, digital privacy, reporting mechanisms including the National Cyber Crime Reporting Portal and intermediary grievance systems and legal remedies available under cyber laws.

Taken together, the Information Technology Act, 2000, the Information Technology Rules, 2021, advisories, the Standard Operating Procedure for NCII, proposed regulatory measures addressing synthetically generated content, the Digital Personal Data Protection Act, 2023, institutional coordination under Mission Shakti and awareness initiatives constitute a comprehensive and evolving framework to safeguard the dignity, privacy and security of women in digital spaces, while ensuring accountability of intermediaries and timely redressal for victims.

*****