

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**LOK SABHA**  
**UNSTARRED QUESTION No. 614**  
TO BE ANSWERED ON 22.07.2026

**MISUSING OF AI-BASED IMAGE GENERATION PLATFORMS**

†614. **DR. ANAND KUMAR:**

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

- (a) whether the Government is aware that by misusing Artificial Intelligence (AI) based image generation platforms, photos of individuals especially women and children are being altered to create objectionable and obscene image thereby posing a serious threat to their privacy, dignity and safety;
- (b) the number of such cases registered during the last three years and the number of FIRs registered in such cases along with the number of cases in which action has been taken by the Government;
- (c) whether the Government has issued any specific guidelines/rules related to the IT Act, cyber laws or AI to prevent such misuse and if so, the details thereof; and
- (d) whether the Government is proposing to introduce more stringent regulatory mechanism to fix the accountability of AI platforms to provide immediate relief to victims and to ensure the prompt removal of such objectionable content?

**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, including women and children. The Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, together, have put in place a stringent framework to deal with unlawful and harmful content in the digital space.

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

The IT Act provides punishment for various cyber offences such as identity theft (section 66C), impersonation (section 66D), privacy violations (section 66E), publishing or transmitting obscene or sexually explicit content (sections 67, 67A, 67B). It also empowers Police to investigate offences (Section 78 and 80).

**IT (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 is harmful to children, obscene, pornographic, invasive of another’s privacy, insulting or harassing on the basis of gender or violates any law for the time being in force.

The intermediary, within two hours from the receipt of a complaint made by an individual or any person on behalf, in relation to any content which involves full / partial nudity, exposing the private area and artificially morphed images of an individual should take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.

### **Recent amendments:**

Recent amendments to IT Rules require social media platforms and other intermediaries to remove unlawful content within three hours of the receipt of an order of a court of competent jurisdiction or reasoned intimation by the Appropriate Government or its agency.

Intermediaries, in cases where the violation involves the commission of an offence under any law currently in force—such as the Bharatiya Nyaya Sanhita, 2023 read with the Bharatiya Nagarik Suraksha Sanhita, 2023, or the Protection of Children from Sexual Offences Act, 2012, which mandates reporting must report such offence to the appropriate authority in accordance with the provisions of the applicable law.

On 10<sup>th</sup> February, 2026, the Government strengthened the regulatory framework by amending the IT Rules, 2021 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.

**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:

- Vide Advisory dated 29.12.2025, government reiterated to the intermediaries regarding observance of statutory due diligence obligations under the IT Act and IT Rules, for preventing hosting, publication, transmission, sharing or uploading of vulgar, indecent, obscene, pornographic and other unlawful content on their platforms. It also advised the intermediaries to undertake an immediate review of their internal compliance frameworks, content moderation practices and user enforcement mechanisms, and to ensure strict and continuous adherence to the provisions of the IT Act and the IT Rules.
- 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.

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication “Crime in India”. The latest published report may be accessed on <https://ncrb.gov.in>

‘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).

\*\*\*\*\*