GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 2456
TO BE ANSWERED ON: 21.03.2025

IMPROVEMENT IN CSAM REPORTING UNDER SAHYOG PLATFORM

2456. SMT. REKHA SHARMA:
SHRI MADAN RATHORE:
SMT. KIRAN CHOUDHRY:
SMT. MAYA NAROLIYA:
SHRI BABURAM NISHAD:
SHRI IRANNA KADADI:
DR. MEDHA VISHRAM KULKARNI:

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

(a) the specific measures proposed under the Sahyog platform, and the manner in which it will improve direct Child Sexual Abuse Material (CSAM) reporting to law enforcement;
(b) whether Government has developed monitoring mechanisms to ensure that social media platforms do not delay, suppress, or under-report CSAM cases;
(c) whether the Intermediary Guidelines (IT Rules), 2021 will be amended to introduce stricter obligations for tech platforms on CSAM reporting and takedown; and
(d) the current status of the Sahyog platform, and whether it has been deployed for testing or pilot implementation?

ANSWER

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

(a) to (d): The policies of the Central Government are aimed at ensuring an open, safe, trusted and accountable Internet for its users.

The Information Technology Act, 2000 ("IT Act") provides punishment for publishing or transmitting obscene material and material containing sexually explicit act in electronic form.The IT Act also provides stringent punishment for publishing or transmitting of material depicting children in sexually explicit act in electronic form.Such anoffence is punishable with imprisonment of up to five years on first conviction and sevenyears on subsequent conviction along with fine, and is a cognizableoffence. Further, as per the Bharatiya Nagarik Suraksha Sanhita (BNSS), prevention and investigation of cognizable offences is to be done by the police and since 'Police' is a State subject under the Seventh Schedule to the Constitution, States are primarily responsible for the prevention, investigation etc. of such cybercrime against children. Accordingly, State police departments take preventive and penal action as per law in respect of any cybercrime against children.

Additionally, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules") cast specific obligations on intermediaries, including social media intermediaries, to observe due diligence while discharging its duties.Such obligations include the making of reasonable efforts by the intermediary to cause its users not to host, display, upload, publish, transmit or store any information that knowingly or intentionally violates any law. Intermediaries are also obligated to remove,within 24 hoursfrom the receipt of a complaint made by an individual or any person on his behalf,any content which prima facie exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct. Also, in case a significant social media intermediary is providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its

computer resource for the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to child sexual abuse material. Further, intermediaries, including social media intermediaries, are obligated to remove any information violative of any law in India as and when brought to their knowledge either through a court order or through a notice by an appropriate government or its authorized agency.

To further strengthen the mechanism to deal with such cybercrimes in a coordinated manner, the Government has also taken several other measures, including the following:

(i) The Ministry of Home Affairs (MHA) operates a National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable citizens to report complaints pertaining to all types of cybercrimes, with special focus on cybercrimes against children. Indian Cyber Crime Coordination Centre (I4C), an attached office to MHA, has also been set up the to deal with all types of cybercrime, including cybercrime against children, in a coordinated and comprehensive manner.

(ii) To streamline the process of issuing takedown notices for removal of unlawful information, I4C in collaboration with Ministry of Home Affairs, Ministry of Electronics and Information Technology and Department of Telecommunications has developed a dedicated portal called Sahyog. The Sahyog Portal has been launched to automate the process of sending notices to intermediaries by the Appropriate Government or its agency under section 79(3)(b) of the IT Act to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act. The portal has been developed to bring together all Authorized Agencies of the countryand intermediaries on a single platform for ensuring immediate action against the unlawful online information to achieve a safe cyber space for the citizens of India.

(iii) An MoU has been signed between the National Crimes Record Bureau (NCRB), MHA and National Center for Missing and Exploited Children (NCMEC), USA regarding sharing of Tipline reports on online child explicit material and child sexual exploitation content. The Tiplines, as received from NCMEC, are being shared withLaw Enforcement Agencies (LEAs) of States/UTs online through the National Cybercrime Reporting Portalfor taking further legal action as per the provision of law against the offenders.

(iv) The Government periodically blocks the websites containing child sexual abuse material (CSAM) based on INTERPOL's "worst of list" received.

****