GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 408
TO BE ANSWERED ON: 09.12.2022

CURBING OF OBSCENITY AND VULGARITY ON SOCIAL MEDIA NETWORKS

408. DR. KANIMOZHI NVN SOMU:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) the stringent steps taken by Government to curb and stop the prevalence of obscenity and vulgarity in the name of web series on social media networks; and

(b) whether it is possible for Government to stop the prevalence of obscenity and vulgarity on social media networks through the existing IT laws and Acts and to punish the perpetrators, if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. With the expansion of the Internet and more and more Indians coming online, the potential for Indians being exposed to obscene and vulgar content on the Internet has grown. The many challenges in securing cyberspace also flow from its vastness and borderless nature.

The Information Technology Act, 2000 ("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), and makes them punishable with imprisonment for a period that may extend to three and five years respectively, and as per section 77B such cybercrimes are cognizable offences. As per the provisions of the Code of Criminal Procedure, 1973, prevention and investigation of cognizable offences is to be done by the police, and as per the Seventh Schedule to the Constitution, 'Police' is a State subject. As such, States are primarily responsible for the prevention, investigation etc. of such cybercrimes through the State police departments, which take preventive and penal action as per law, including in respect of the said cybercrimes pertaining to publishing or transmitting of material containing sexually explicit act or obscene material in electronic form.

To help achieve the aim of making Internet Open, Safe and Trusted and Accountable and to strengthen the mechanism to deal with such cybercrimes in a coordinated manner,the Central Government, in exercise of powers conferred by the IT Act, has made the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. These rules cast specific obligation on intermediaries, including social media intermediaries, to observe due diligence and provide that if they fail to observe such due diligence, they shall no longer be exempt from their liability under law for third-party information or data or communication link hosted by them. Such due diligence includes the following:

(i) To make reasonable efforts to cause the users not to host, display, upload, modify, publish, transmit, store, update or share, among others, information which is obscene, or paedophilic, or pornographic, or is invasive of another's bodily privacy, or is harmful to child, or impersonates another person, or violates any law;

(ii) To provide, upon receipt of an order from a lawfully authorised government agency, information or assistance for prevention, detection, investigation or prosecution under law;

(iii) To have in place a grievance redressal machinery, and resolve complaints of violation of the rules within 72 hours of being reported and, in case of a complaint by an individual or her/his authorised representative, remove within 24 hours 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, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual;

(iv) In case an intermediary is a significant social media intermediary (*i.e.*, an intermediary having more than 50 lakh registered users in India), to additionally observe due diligence in terms of appointing a Chief Compliance Officer, a nodal contact person for 24x7 coordination with law enforcement agencies and a Resident Grievance Officer.

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 operates a National Cyber Crime Reporting Portal (www.cybercrime.gov.in) and a toll-free number (1930) to enable citizens to report complaints pertaining to all types of cybercrimes, with special focus on cybercrimes against children. The Ministry has also set up the Indian Cyber Crime Coordination Centre (I4C) to deal with all types of cybercrime, including cybercrime against children, in a coordinated and comprehensive manner.

(ii) The Ministry of Home Affairs has provided financial assistance to States and Union territories under the Cyber Crime Prevention against Women and Children Scheme for capacity building, including for the setting up of cyber forensic-cum-training laboratories and training of personnel of law enforcement agencies, public prosecutors and judicial officers. So far, cyber forensic-cum-training laboratories have been commissioned in 30 States and Union territories.

(iii) Government from time-to-time has blocked websites containing child sexual abuse material (CSAM), based on lists from Interpol received through the Central Bureau of Investigation, India's national nodal agency for Interpol.

(iv) Government has issued an order to Internet Service Providers, directing them to implement Internet Watch Foundation, UK or Project Arachnid, Canada list of CSAM websites/webpages on a dynamic basis and block access to such web pages or websites.

(v) The Department of Telecommunications has requested Internet Service Providers (ISPs) to spread awareness among their subscribers about the use of parental control filters, and has also directed ISPs with International Long Distance license to block certain websites found to be containing CSAM.

(vi) The Central Board of Secondary Education has issued guidelines on 18.8.2017 to schools on the safe and secure use of Internet. These guidelines direct schools to install effective firewalls, filtering and monitoring software mechanisms in all computers and to deploy effective security policies.

(vii) To spread awareness on cybercrime, the Ministry of Home Affairs has taken several steps that include dissemination of messages on cybercrime through the Twitter handle @cyberDost, radio campaigns and publishing of a Handbook for Adolescents/Students.

(viii) The Ministry of Electronics and Information Technology is implementing the Information Security Education and Awareness (ISEA) Phase-II project to build capacities in the area of information security, train government personnel and create mass information security awareness for users. Under this, a large number of awareness workshops have been conducted across the country, school teachers trained as master trainers to reach out to crores of users in the indirect mode through Cyber Safety and Cyber Security Awareness Weeks organised in select cities in collaboration with State Cyber Cell / Police departments, mass awareness

programmes broadcasted through Doordarshan / All India Radio, bimonthly newsletters published in print and digital mode, and multilingual awareness content in the form of handbooks, multimedia short videos, posters etc., which have been disseminated through print, electronic and social media and made available for download on the ISEA awareness portal (www.infosecawareness.in).

(ix) A memorandum of understanding has been signed between India's National Crime Records Bureau and the National Center for Missing and Exploited Children of the United States of America, for sharing of tipline reports on online child explicit material and child sexual exploitation contents from the said Center. The tip lines, as received from the Center, are shared online with States and Union territories through the National Cybercrime Reporting Portal for further action.

******