GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3357
TO BE ANSWERED ON 09.08.2023

CIRCULATION OF CSAM

3357. SHRI A. RAJA:

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

(a) whether the Government has taken cognizance of increase in the circulation of Child Sexual Abuse Materials (CSAM) and pornographic materials in the cyber space and if so, the details thereof;
(b) the total number of registered cases filed in this regard during the last three years;
(c) the total number of cases in which stringent action was taken including blocking of the site; and
(d) the steps taken or proposed to be taken to prevent the spread of CSAM and pornographic materials on the internet?

ANSWER

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

(a): The policies of the Government are aimed at ensuring a Safe and Trusted and Accountable Internet for all its users.

Publication or transmission of electronic material depicting children in sexually explicit act, is cybercrime. The Central Government is taking zero tolerance policy towards any such cybercrimes.

The Information Technology Act, 2000 ("IT Act") and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021"), provides for penalty and punishment for such act and also casts an obligations on the intermediaries, including social media intermediaries, to observe due diligence as per rule 3(1)(b) and 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 that 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 rape, sexually explicit material or child sexual abuse material.

(b): As per the data maintained by National Crime Records Bureau, cases registered under the sub-category Cyber Pornography/Hosting or Publishing Obscene Sexual Materials depicting children, under the category Cyber Crimes against Children, are 102, 735 and 969 for the year 2019, 2020 and 2021, respectively.

(c) to (d): The Information Technology Act, 2000 ("IT Act") and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021"), together, have made a framework which cast obligations on the 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, information which is harmful to child, or obscene, or invasive of another's bodily privacy, or violates any law;
(ii) On a voluntary basis on violation of the above, and on actual knowledge upon receipt of a grievance or court order or notice from the appropriate government or its agency, to not host, store or publish unlawful information prohibited under law for the time being in force in relation to the interest of decency or morality or defamation;

(iii) Upon receipt of an order from a lawfully authorised government agency, to provide information or assistance for prevention, detection, investigation or prosecution under law in a timebound manner within 72 hours;

(iv) 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; further, the rules have been amended on 28.10.2022 to provide for the establishment of one or more Grievance Appellate Committee(s) to allow users to appeal against decisions taken by Grievance Officers on such complaints;

(v) 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, and to endeavour to deploy technology-based measures, including automated tools or other mechanisms, to proactively identify information that depicts any act or simulation in any form depicting child sexual abuse or conduct.

(vi) 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 rape, sexually explicit material or child sexual abuse material.

Keeping in view complaints regarding action or inaction, on the part of the social media intermediaries and other intermediaries on user grievances regarding objectionable content or suspension of their accounts, the Central Government has also established three Grievance Appellate Committees (GACs), as provided for in the said IT Rules, 2021 to enable users to appeal against the decisions taken by Grievance Officer of intermediaries on user complaints.

It is further informed that section 67B of the IT Act penalises the publishing or transmitting of electronic material depicting children in sexually explicit act, the creation of text or images, collection, seeking, browsing, downloading, advertising, promotion, exchange or distribution of electronic material depicting them in obscene or indecent or sexually explicit manner, cultivating or enticing or inducing them to online relationship with other children for sexually explicit act or in an offending manner, facilitating their online abuse, and electronically recording abuse pertaining to sexually explicit act with children. Such an offence is punishable with imprisonment of up to five years on first conviction and seven years on subsequent conviction along with fine of up to ten lakh rupees, and is a cognizable offence. Since, as per the Code of Criminal Procedure, 1973, prevention and investigation of cognizable offences is to be done by the police and '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 cybercrime against children.

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) 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 has from time to time 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.

****