GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO.*16
TO BE ANSWERED ON: 07.12.2022

CYBER CRIME AGAINST CHILDREN

***16. SHRIMATI RAJASHREE MALLICK:**
DR. NISHIKANT DUBEY:

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

(a) whether cyber crimes against children have increased during the last two years and if so, the details of the steps being taken by the Government to check the same;

(b) the details of the steps taken by the Government to tackle several confidentiality related risks to children like cyber threat and online harassment; and

(c) the details of various steps taken to check fake calls, fake messages, etc.?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (c): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN THE REPLY TO LOK SABHA STARRED QUESTION NO. *16 FOR 07.12.2022, REGARDING CYBER CRIMES AGAINST CHILDREN

……

As per data published by the National Crime Records Bureau, 1,102 and 1,376 cases of cybercrime against children were registered during the years 2020 and 2021 respectively.

The Information Technology Act, 2000 ("IT Act") and rules made thereunder contain provisions aimed at making cyberspace safe and accountable for children.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.

Further, 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. With a view to enhance the safety of cyberspace and strengthen the mechanism to deal with such cybercrimes in a coordinated manner, these rules require intermediaries to observe, among others, diligence as under:

(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;

(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.

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.

With regard to fake calls, fake messages, etc., it is informed that section 66D of the IT Act penalises cheating by impersonating by means of any communication device or computer resource and the same is punishable with imprisonment of up to three years and fine of up to one lakh rupees. As the offence is a cognizable offence, State police departments take preventive and penal action as per law in respect of the same. Further, the Information Technology (Intermediary

Guidelines and Digital Media Ethics Code) Rules, 2021 require intermediaries to observe, among others, diligence to make reasonable efforts to cause the users not to host, display, upload, modify, publish, transmit, store, update or share, information which deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature, or impersonates another person. Further, other due diligence as applicable in respect of cybercrimes against children is also applicable in respect of information, misinformation or impersonation as said.

****