GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO.*144
TO BE ANSWERED ON: 08.12.2021

CYBER CRIMES AGAINST CHILDREN

***144. SHRI KANAKMAL KATARA:**
SHRIMATI KESHARI DEVI PATEL:

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

(a) whether cyber crimes against children haveincreased during the last two years and if so, the detailsof steps being taken by the Government to check thesame;
(b) the details of steps taken by the Government totackle several confidentiality related risks to children likecyber threat and online harassment; and
(c) the details of various steps taken to check fakecalls, 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 REPLY TO LOK SABHA STARRED QUESTION NO. *144 FOR08-12-2021 REGARDINGCYBER CRIMES AGAINST CHILDREN

……..

(a) and (b): With the expansion of internet and more and more Indians coming online, the incidents of cyber crimes including crimes against children online is also increasing. The challenges of cyber space are many which flow from its vastness and borderless character. That is why the government is committed to policies and actions that ensure that Internet in India is always Open, Safe & Trusted and Accountable for all Indians. The National Crime Records Bureau (NCRB) compiles and publishes statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2020. As per data published by NCRB, a total of 306 and 1102 cases of cyber crime against children were registered during the year 2019 and 2020 respectively.

'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes through their Law Enforcement Agencies (LEAs). The LEAs take legal action as per provisions of law against the offenders.

To strengthen the mechanism to deal with cyber crimes including crimes against children in a comprehensive and coordinated manner, the Central Government has taken measures in consultation with various stakeholders which, inter-alia, include the following:

(i) Section 67B of the Information Technology (IT) Act, 2000 provides stringent punishment for publishing, transmitting or viewing Child sexual abuse material online.

(ii) The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 empower the users of Intermediaries and makes the social media platforms accountable for their safety. The Rules require the intermediaries to adopt a robust grievance redressal mechanism including time-bound disposal of grievances. The Intermediaries need to convey their terms and conditions which must include communication to users not to host, display, upload, modify, publish, transmit, update or share any information that is inter alia harmful, defamatory, obscene, invasive of another's privacy, harm minors in any way or are otherwise unlawful. Intermediaries are also expected 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 authorised agency. The Rules also require Significant Social media Intermediary (SSMI) to endeavour to deploy technology based measures to proactively identify child sexual abuse material.

(iii) 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 cyber crimes with special focus on cyber crimes against women and children. Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre (I4C)' to deal with all types of cyber crime in the country, in a coordinated and comprehensive manner.

(iv) Government periodically blocks the websites containing extreme child sexual abuse material (CSAM) based on INTERPOL's "worst of list" received through Central Bureau of Investigation (CBI), the national nodal agency for Interpol in India.

(v) Government has issued an order to concerned Internet Service Providers (ISPs) ordering them to implement Internet Watch Foundation (IWF), UK or Project Arachnid, Canada list of CSAM websites/webpages on a dynamic basis and block access to such child pornography webpages/websites.

(vi) DoT has requested all Internet Service Providers (ISPs) to make suitable arrangement to spread awareness among their subscribers about the use of parental control filters in the end-user machines through messages of email, invoices, SMS, website, etc.

(vii) Central Board of Secondary Education (CBSE) has issued guidelines on 18.08.2017 to schools on the safe and secure use of Internet. This circular directs schools to install effective firewalls, filtering and monitoring software mechanisms in all the computers and deploy effective security policies.

(viii) To spread awareness on cybercrime, MHA has taken several steps that include dissemination of messages on cybercrime through Twitter handle @cyberDost, radio campaign, publishing of Handbook for Adolescents / Students.

(ix) MeitY through a program, namely, Information Security Education & Awareness (ISEA), has been creating awareness among users including women and children highlighting the importance of digital safety while using Internet. A dedicated website for information security awareness (https://www.infosecawareness.in) provides relevant awareness material.

(x) A MoU is signed between the NCRB, India and National Center for Missing and Exploited Children (NCMEC), USA regarding receiving of Tipline report on online child pornography and child sexual exploitation contents from NCMEC. The Tip lines, as received from NCMEC, are being shared with Stats/UTs online through Nation Cybercrime Reporting Portal for taking further action.

(c): The Information Technology (IT) Act, 2000 has a provision to deal with menace of fake calls and messages made through internet as medium. Section 66D of the IT Act, 2000 provides for punishment of imprisonment up to three years and fine for cheating by personation.

******