

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2491
TO BE ANSWERED ON: 01.08.2018

CYBER BULLYING

2491. SHRI K.C. VENUGOPAL:

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

- (a) the details of action taken by the Government to curtail the growing incidents of cyber bullying and blackmail and if so, the details thereof;
- (b) whether the Government has formulated any comprehensive mechanism to curb and monitor cyber crimes in the country;
- (c) if so, the details thereof;
- (d) whether the Government has taken any measures to stop the incidents of circulation of videos of sexually abused children and women through social media; and
- (e) if so, the details and the status thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a): The Information Technology (IT) Act, 2000 has adequate provisions to deal with prevailing cyber crimes. Further, sections 354A and 354D of Indian Penal Code provides punishment for cyber bullying and cyber stalking. Ministry of Home Affairs has issued an Advisory on 4.1.2012 on Preventing & combating Cyber Crime against Women and Children, wherein it was advised to States/Union Territories to specifically combat the crimes in forms of cyber stalking, cyber bullying, child pornography and exposure to sexually explicit material etc.

(b) and (c): Government has taken a number of legal, technical and administrative measures to prevent cyber crimes. These inter alia, include:

- (i) Enactment of IT Act, 2000 which has adequate provisions to deal with prevalent cyber crimes.
- (ii) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of cyber crime cases.
- (iii) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of law enforcement personnel and Judiciary in these States.
- (iv) Government has formulated Cyber Crisis Management Plan for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. Regular workshops

are conducted for Ministries, Departments, States & Union Territories and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan.

- (v) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.
- (vi) Ministry of Home Affairs has issued National Information Security Policy and Guidelines (NISPG) to Government organizations to ensure safety of data and minimize cyber threats.

(d) and (e): The measures taken by Government to address issues relating to transmission/circulation of such objectionable videos are as follows :

- (i) Sections 66E, 67, 67A and 67B of the IT Act 2000 provides punishment for uploading/transmissions of videos of sexual abuse including child pornography.
- (ii) Ministry of Home Affairs (MHA) has launched a portal www.cybercrime.gov.in for public to report complaints of child pornography and sexually abusive explicit content.
- (iii) In addition, Protection of Children from Sexual Offences Act (POCSO) E-box portal by National Commission for Protection of Child Rights (NCPCR) was opened for reporting of cyber crime targeting children. NCPCR has now enhanced the scope of POCSO E-box to also handle cyber bullying, cyber stalking, morphing of images and child pornography. The E-Box is also available as Mobile app at Google/Apple Play Store.
- (iv) Government periodically blocks the websites containing extreme Child sexual abuse material based on INTERPOL's "worst of list" received through Central Bureau of Investigation (CBI) which is the national nodal agency for INTERPOL in India. As on date a total of 4934 websites have been ordered for blocking through Internet Service providers (ISPs).
- (v) Government has issued an order to concerned ISPs to adopt Internet Watch Foundation (IWF) list of CSAM websites/webpages and block access to child pornography webpages/ websites at gateway level. This dynamic list is updated daily.
- (vi) DoT has communicated to all ISPs requesting them 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
