

**GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA**

UNSTARRED QUESTION NO:231

ANSWERED ON:25.02.2015

CYBER CRIMES AGAINST WOMEN AND CHILDREN

Bhuria Shri Dileep Singh

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

- (a) whether government has taken any steps to curb the cyber crimes against women & children, and if so, the details thereof?
- (b) whether the government has made or proposes to direct internet service providers to control internet content on child/women abuse and if so, the details thereof?
- (c) whether the government has made or proposes to collaborate with law agencies of other countries and international agencies for investigation in cyber crimes; and
- (d) if so, details thereof.

Answer

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI RAVI SHANKAR PRASAD)

(a): Government has taken various steps comprising legal, technical and of administrative nature to deal with the issues of cyber crimes against women and children. The sections 66A, 66E, 67, 67A, 67B and 69A of the Information Technology Act,, 2000 deals with various aspects of crimes covering those committed against woman and child. Besides amendments were also made in the Indian Penal Code (IPC) to address some of the specific crimes which may be committed through using Information Technology against women. Similarly, the Protection of Children from Sexual Offences Act (POCSO) also deals with cyber related crimes against children. The legal framework is comprehensive and adequately deals with all the issues of cyber crimes against women and children.

The various measures have been taken to enhance the capabilities of law enforcement agencies in the area of investigation of cyber crimes. The specific steps include the following:

- i. Setting up of 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 and Judiciary in these States.
- ii. Cyber Crime Cells set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.
- iii. Industry associations such as Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have taken up tasks of awareness creation and training programmes on Cyber Crime investigation.
- iv. Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are engaged in conducting awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.
- v. More than 26000 Police Officers and 600 judicial officers have so far been trained in the training Labs established by the Government.
- vi. Development of Cyber forensics tools for collection, analysis, presentation of the digital evidence for use by Law Enforcement Agencies.

Presently an expert group consisting of academicians and professionals of repute is engaged in preparing the road-map for tackling cyber crimes in the country.

(b): Under sub-Section (2) of Section 79 of Information Technology Act 2000, the intermediary including internet service providers (ISPs) have statutory obligations to observe due diligence and guidelines prescribed by the Government. The details of the due diligence to be observed by the intermediaries have been prescribed under the Information Technology (Intermediary Guidelines) Rules, 2011 enacted under Section 79 and notified on 13.04.2011. As per sub-Rule 3 (2) of the Rules as above, the intermediaries are required to take necessary action to inform the users not to host, display, upload, modify, publish, transmit, update or share any information which is objectionable in any way (including pornography). Government has also been issuing advisories to the intermediaries to block or remove objectionable material. Government is in regular dialog with intermediaries including social networking sites for effective disablement of such objectionable content.

(c) and (d): Government is regularly engaged with other countries through the bilateral cooperation to collaborate with their law and international agencies for sharing of information relating to crimes including those related to women and children. Further, the provisions of MLAT (Mutual Legal Assistance Treaty) are used for eliciting support for cyber crime cases. United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ) has a mandate to focus on the issues related to cyber crime and related response by the member States.