GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**RAJYA SABHA**
**UNSTARRED QUESTION NO. 389**
TO BE ANSWERED ON 04-02-2021

**WOMEN SAFETY IN THE DIGITAL SPACE**

**389   DR.  NARENDRA  JADHAV:**

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

(a)   in what manner, Government is ensuring the digital safety of citizens particularly women in addition to existing content reporting mechanisms available to users, the details thereof;
(b)   the number of orders served by the Government to social media platforms to take down content hampering the digital safety of citizens, the details thereof ;
(c)   whether the Ministry is maintaining data of sub-judice cases on cyber stalking, bullying and harassment across the country and if so, the details thereof, State wise; and
(d)   whether the Ministry or Ministries of Home Affairs or Women and Child Development had consultation with social Media platforms on these issues, the details thereof?

**ANSWER**

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): 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. As, "Police" and "Public Order" are State subjects, complaints reported on this portal are attended by the respective Law Enforcement Authorities of States/Union Territories. Further any unlawful content can be reported to police station.

MHA has also launched a programme for registration of citizens as 'Cyber Volunteers' on National Cyber Crime Reporting Portal to report for unlawful contents on the websites, social media platforms, etc including contents relating to women and children. Further, Ministry of Electronics and Information Technology (MeitY) works with social media platforms to provide for ease of reporting by users of any abusive, harmful or unlawful content violative of their policy.

Government is committed for digital safety of people and has taken several steps that *inter alia*, include:
(i)   There are adequate legal provisions to deal with digital safety of persons particularly women and children. The Information Technology (IT) Act, 2000 has adequate provisions to deal with prevalent cyber crimes including the ones related to women.  Sections 66E, 67, and 67A of the Act provide for the punishment and fine for violation of bodily privacy and publishing or transmitting of obscene/sexually-explicit material in electronic form. Section 67B of the Act specifically provides stringent punishment for publishing, browsing or transmitting child pornography in electronic form. Further, sections 354C and 354D of Indian Penal Code provide punishment for cyber bullying and cyber stalking.

(ii) Information Technology (Intermediary Guidelines) Rules, 2011 notified under section 79 of the IT Act require that the intermediaries shall observe due diligence while discharging their duties and shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person;  inform their users not to host, display, upload, modify, publish, transmit, update  or share any  information that  is grossly harmful, harassing,  obscene
and invasive of another's privacy or otherwise unlawful in any manner whatsoever.  The intermediary shall publish on its website the name of the Grievance Officer and his contact details to address the grievances received from users and affected individuals / organizations. Intermediaries are also expected to remove any unlawful content relatable to Article 19(2) of the Constitution of India as and when brought to their knowledge either through a court order or through a notice by appropriate government or its agency or as directed under section 69A of the IT Act, 2000.

(iii) 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.

(iv) Government has issued direction to concerned Internet Service Providers (ISPs) to work out a suitable arrangement for receiving Internet Watch Foundation (IWF), UK list of CSAM websites/webpages on a dynamic basis and block access to child pornography webpages/websites.

(v) National Commission for Protection of Child Rights (NCPCR) has published a booklet on "Child Victims of Cyber Crime – Legal Tool Kit" as a guide for investigating officers for better understanding of the cyber crime related laws in simple language.

(vi) MeitY through a program, namely, Information Security Education & Awareness (ISEA), has been creating awareness among users highlighting the importance of following the ethics while using Internet and advising them not to share rumours/fake news. A dedicated website for information security awareness (https://www.infosecawareness.in) provides relevant awareness material. Under the programme, 21 awareness workshops on Information Security exclusively for women have been organized covering 2,083 participants. The topics/content covered in these workshops include cyber security, cyber stalking, online shopping, social media and privacy, password management, internet security, mobile security, browser security, online banking, instant messaging, etc. Besides this, an exclusive handbook namely 'Information Security Awareness handbook for Women', 'Cyber Security tips for Women' and 'Online Safety tips for Women@Home during COVID 19' have been designed. The awareness content designed/developed exclusively for women have been made available for download on the *website* https://www.infosecawareness.in/women.

(vii) MeitY on 20.03.2020 issued an advisory to major social media platforms like Facebook, Twitter, Instagram, YouTube, TikTok and Helo wherein the Intermediaries were urged to:

– initiate awareness campaign on their platforms for the users not to upload/circulate any false news/misinformation concerning corona virus which are likely to create panic among public and disturb the public order and social tranquillity;
– take immediate action to disable /remove such content hosted on their platforms on priority basis;
– promote dissemination of authentic information related to corona virus as far as possible.

(b): Section 69A of the IT Act empowers Government to block any information generated, transmitted, received, stored or hosted in any computer resource in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commissioning of any cognizable offence relating to above. The no. of websites/ webpages/ accounts blocked during the last 3 years are as follows :

| Year | No. of websites/webpages/accounts Blocked |
|------|-------------------------------------------|
| 2018 | 2799 |
| 2019 | 3635 |
| 2020 | 9849 |

The power for blocking of information for public access is vested with Central Govt. and thus data for State/UT is not applicable.

(c): MeitY does not maintain data of sub-judice cases on cyber stalking, bullying and harassment.

(d): MeitY and Ministry of Home Affairs regularly interacts with social media platforms on issues related to spreading of fake news, misinformation/disinformation on Internet. Ministry of Women and Child Development also interact with social media platforms on the issue of digital safety of women and children. Social media platforms have implemented a number of steps to address these issue.

********