GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 852

TO BE ANSWERED ON THE 14TH DECEMBER, 2022/ AGRAHAYANA 23, 1944 (SAKA)

CYBER CRIME AGAINST WOMEN

852. SHRI SANJEEV ARORA:

Will the Minister of HOME AFFAIRS be pleased to state:

the strategy to address the increasing trend in cyber crime against women in light of the increasing incidents of abuse, indecency, stalking, impersonation, theft etc?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI AJAY KUMAR MISHRA)

'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 including cyber crime against women through their Law Enforcement Agencies (LEAs).

The Central Government has taken various measures to supplement the efforts of States/UTs to deal with cybercrimes against women which, inter-alia include the following:

i. **The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre (I4C)' to provide ecosystem for tackling all types of**

cyber crime in the country, in a coordinated and comprehensive manner.

ii. The Ministry of Home Affairs has provided financial assistance under the 'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs' personnel, public prosecutors and judicial officers. So far, cyber forensic-cum-training laboratories have been commissioned in 30 States/UTs.

iii. Training curriculum has been prepared for Law Enforcement Agencies personnel, prosecutors and judicial officers for better handling of investigation and prosecution. States/UTs have been mandated to organize training programmes. So far, more than 20,000 LEA personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc.

iv. Ministry of Home Affairs operationalized the National Cyber Crime Reporting Portal www.cybercrime.gov.in to provide a centralized mechanism to the citizens for online reporting of all types of cyber crime incidents, with a special focus on cyber crimes against women and children. Incidents reported on this portal are automatically routed to the State/UT law enforcement agency concerned for taking further steps as per the provisions of the law. A toll-free helpline number '1930'

has been operationalized to get assistance in lodging online cyber complaints.

v. The Massive Open Online Courses (MOOC) platform under the I4C called 'CyTrain' portal has been developed. CyTrain portal helps in the capacity building of Police Officers/Judicial Officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. along with certification. So far, more than 27,900 Police Officers from States/UTs are registered and more than 7,300 Certificates issued through the portal.

vi. The Information Technology Act, 2000 ("IT Act") and rules made there under contain several provisions for safeguarding users in the cyberspace. The IT Act penalizes various cybercrimes relating to computer resources, including dishonestly or fraudulently accessing a computer resource without the permission of its owner commonly referred to as hacking (section 66), identity theft (section 66C), cheating by impersonation (section 66D), violation of bodily privacy (section 66E), transmitting of obscene material (section 67), and publishing or transmission of material containing sexually explicit act in electronic form (section 67A and 67B) and tampering with computer Source documents (section 65), etc. Each such cybercrime is

punishable with imprisonment for a period that may extend to either three years or five years, and as per section 77B of the IT Act such cybercrimes are cognizable offences.

To help make cyberspace safe, trusted and accountable, 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, which require intermediaries, including social media intermediaries, to observe, among others, diligence as under:

- **To publish on their website and app, their rules and regulations, privacy policy and user agreement;**
- **To inform the said rules to their users and to make reasonable efforts to cause the users not to host, display, upload, modify, publish, transmit, store, update or share, certain types of malicious of information.**
- **To have in place a grievance redressal machinery, and resolve complaints of violation of the rules within 72 hours of being reported;**

Further, it has notified amendments to these rules 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.

vii. To spread awareness on cyber crime, several steps have been taken that include issuance of alerts/ advisories, dissemination of messages through SMS, I4C social media account i.e. Twitter handle (@Cyberdost), Facebook (CyberDostI4C), Instagram (cyberdosti4c), Telegram (cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple media, publishing of Handbook for Adolescents/ Students, organizing of Cyber Safety and Security Awareness week, in association with police department in different States/ UTs etc.

****