GOVERNMENT OF INDIA MINISTRY OF HOME AFFAIRS

LOK SABHA UNSTARRED QUESTION NO. 2944

TO BE ANSWERED ON THE 18TH MARCH, 2025/ PHALGUNA 27, 1946 (SAKA)

CYBERCRIME AGAINST WOMEN

2944. MS SAYANI GHOSH:

Will the Minister of HOME AFFAIRS be pleased to state:

- (a) the total number of cybercrime complaints related to crimes against women registered on the National Cyber Crime Reporting Portal in the last five years, year-wise;
- (b) the breakup of these complaints, including cyberstalking, online harassment, cyber blackmailing, identity theft, Non-Consensual Intimate Content (NCIC), deepfake misuse, and other offences, category-wise;
- (c) the number of cases resolved and pending, and the average time taken for resolution of complaints related to women, State-wise; and
- (d) whether the Government is taking any steps to strengthen digital safety measures for women, including stricter enforcement, awareness campaigns and Al-based monitoring, if so, the details thereof?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS (SHRI BANDI SANJAY KUMAR)

(a) to (d): 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The 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 supplements

the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

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

- i. 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.
- ii. Cyber Forensic-cum-Training Laboratories have been commissioned in 33 States/UTs. As per available information, Cyber Forensic-cum-Training Laboratory has not been established in Tamil Nadu under CCPWC scheme.
- iii. Training curriculum has been prepared for LEA personnel, Public Prosecutors and Judicial officers for better handling of investigation and prosecution. States/UTs have been requested to organize training programmes. More than 24,600 LEA personnel, Public Prosecutors and

Judicial officers have been provided training on cyber crime awareness, investigation, forensics etc. under CCPWC Scheme.

- iv. The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.
- Reporting (NCRP) The **'National** Cyber Crime Portal' v. (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law. The total number of cybercrime incidents related to crimes against women reported on the NCRP in the last five years are as under:

Category	Sub-Category	2020	2021	2022	2023	2024
CSAM/CSEM/RG R (Anonymous + Report &Track)	Child Pornography (CP)- Child Sexual Abuse Material (CSAM)	2019	2109	3062	2957	6079
	Rape/Gang Rape (RGR)- Sexually Abusive Content	2184	27945	30574	12129	4273
	Sexually Obscene material	9606	12251	16341	14322	21990
	Sexually Explicit Act	8379	9743	12247	10658	16133
TOTAL		22188	52048	62224	40066	48475

Incidents reported in the categories like Cyberstalking, Identity Theft etc. in another category of 'Online and Social Media related Crime' on NCRP for the last five years are as under:

Category	Sub-Category	2020	2021	2022	2023	2024
Online and Social Media Related Crime	E-Mail Phishing	897	798	1364	1272	2009
	Cheating by Impersonation	9808	12617	20041	18135	19989
	Fake/Impersonating Profile	12310	15843	23626	30234	39846
	Profile Hacking/ Identity Theft	10419	10650	26288	33724	38295
	Provocative Speech for unlawful acts	5237	2320	4092	3597	5250
	Impersonating Email	225	208	285	304	586
	Intimidating Email	245	149	227	228	571
	Online Job Fraud	4973	7504	10292	13764	10461
	Online Matrimonial Fraud	528	623	1149	926	854
	Cyber Bullying / Stalking / Sexting	11641	21589	44270	39080	39077
TOTAL		56283	72301	131634	141264	156938

vi. In exercise of the powers conferred by clause (b) of sub-section (3) of section 79 of the Information Technology Act 2000, Central Government being the appropriate government designated the Indian Cyber Crime Coordination Centre (I4C), to be the agency of the Ministry of Home Affairs to perform the functions under clause (b) of sub-section (3) of section 79 of Information Technology Act, 2000 and to notify the instances of information, data or communication link residing in or connected to a computer resource controlled by the intermediary being used to commit the unlawful act on 13.03.2024.

- vii. National Cyber Forensic Laboratory (Evidence) was inaugurated on 14.05.2022 at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and reduced turnaround time by 50%.
- viii. The state of the art 'National Cyber Forensic Laboratory (Investigation)' has been established, as a part of the I4C, at New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) has provided its services to State/UT LEAs in around 11,835 cases pertaining to cyber crimes.
 - ix. The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. More than 1,02,321 Police Officers from States/UTs are registered and more than 79,909 Certificates issued through the portal.
 - x. A State of the Art Centre, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law

Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.

- xi. Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by on boarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh.
- Xii. Samanvaya Platform has been made operational to serve as an Management Information System(MIS) platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics based interstate linkages of crimes and criminals, involved in cybercrime complaints in various States/UTs. The module 'Pratibimb' maps locations of criminals and crime infrastructure on a map to give visibility to jurisdictional officers. The module also facilitates seeking and receiving of techno-legal assistance by Law Enforcement Agencies from I4C and other SMEs. It has lead to arrest of 6,046 accused, 17,185 linkages and 36,296 Cyber

Investigation assistance request.

- xiii. 'Sahyog' Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act.
- xiv. To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c), Radio campaign, caller tune, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, newspaper advertisement on digital arrest scam, announcement in Delhi metros on digital arrest and other modus operandi of cyber criminals, use of social media influencers to create special posts on digital arrest, digital displays on railway stations and airports across, etc.
