GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3266
TO BE ANSWERED ON 23.03.2022

CYBER CRIMES AGAINST WOMEN

3266. SHRI ANTO ANTONY:

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

(a) the number of reported cyber-crimes committed against women and children during the pandemic, State-wise and from Year 2020;
(b) whether the Government is taking any special measures for prevention of cyber-crimes against children and women and if so, the details thereof;
(c) whether the Government intends to train law enforcement agencies to handle digital forensics and investigate cyber crimes specifically against women and children and if so, the details thereof and if not, the reasons thereon; and
(d) whether the Government has set up any committee or agency to tackle the rising cyber crimes against children and if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The National Crime Records Bureau (NCRB) compiles and publishes statistical data on crimes in its publication "Crime in India". The latest published report is for the year 2020. As per data published by NCRB, during the year 2020, a total of 1,102 and 10,405 cases of cyber crime against children and women were registered, respectively. The state-wise data for the year 2020 is at Annexure-I.

(b):'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 through their Law Enforcement Agencies (LEAs). The LEAs take legal action as per provisions of law against the offenders.

To strengthen the mechanism to deal with cyber crimes including crimes against women and children in a coordinated manner, the Central Government has taken several measures in consultation with various stakeholders which, *inter-alia*, include the following:

(i) The Information Technology (IT) Act, 2000 has provisions to deal with prevalent cyber crimes including the ones related to women and children. 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 sexually explicit imagery in electronic form. Further, sections 354C and 354D of Indian Penal Code provide punishment for cyber bullying and cyber stalking.

(ii)　The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 empower the users of Intermediaries and makes the social media platforms accountable for users' safety. The Rules *inter alia* provide for

- Expeditious removal of any revenge porn and such other similar content
- Significant Social media Intermediary (SSMI) to deploy technology based measures to proactively identify child sexual abuse material.
- A robust grievance redressal mechanism.

(iii)　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.

(iv)　Internet Service Providers (ISPs) have been directed to block CSAM on a daily basis based on list made available by Internet Watch Foundation (IWF), UK or Project Arachnid, Canada. ISPs also block websites containing extreme child sexual abuse material (CSAM) based on INTERPOL's "worst of list" provided by the government, through Central Bureau of Investigation (CBI), the national nodal agency for Interpol in India.

(v)　Department of Telecom (DoT) has requested all Internet Service Providers (ISPs) 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.

(vi)　To spread awareness on cybercrime, MHA has taken several steps that include dissemination of messages on cybercrime through Twitter handle @cyberDost, radio campaign, publishing of Handbook for Adolescents / Students.

(vii)　MeitY through a program, namely, Information Security Education & Awareness (ISEA), has been creating awareness among users including women and children highlighting the importance of digital safety while using Internet. A dedicated website for information security awareness (https://www.infosecawareness.in) provides relevant awareness material.

Besides conducting training and awareness workshop including those exclusively for women, ISEA has published 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'. The awareness content designed/developed exclusively for women   are   available   for   download   on   the   *website* https://www.infosecawareness.in/women.

(viii)　A MoU has been signed between the NCRB, India and National Center for Missing and Exploited Children (NCMEC), USA regarding receiving of Tipline report on online child pornography and child sexual exploitation contents from NCMEC. The Tip lines, as received from NCMEC, are being shared with Stats/UTs online through Nation Cybercrime Reporting Portal for taking further action.

(c): In order to ensure Safe & Trusted Internet for all its users, MeitY has initiated many projects like Setting up of a Collaborative and Comprehensive Live Cyber Operations Specific Exercise Training Facility (Cyber Closet) for Indian Cyber Space, Development of Cyber Forensic Training cum Investigation Labs in North-Eastern States and Cloud based centralized Cyber Forensics Lab Infrastructures and Capacity Development on Smart Device Forensics Investigations and Creation of Resource Centre for the North Eastern Police Forces. MeitY is already conducting a capacity building programme on cyber laws, crime investigation and digital forensics through Learning Management System

A 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 cybercrime investigation, forensics, prosecution etc. along with certification. More than 11,200 Police Officers from States/UTs are registered and more than 2750 Certificates issued through the portal. MHA has also provided financial assistance to the tune of Rs. 96.13 crore under Cyber Crime Prevention against Women and Children (CCPWC) Scheme to the States/UTs. for setting up of cyber forensic-cum-training laboratories and capacity building of Law Enforcement Agencies (LEAs), public prosecutors and judicial officers. Cyber forensic-cum-training laboratories have been commissioned in 28 States/UTs including Gujarat. 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 19,600 LEA personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc. under CCPWC Scheme.

(d): Government has already created a special body namely The National Commission for Protection of Child Rights (NCPCR) under the administrative control of the Ministry of Women & Child Development. The Commission's Mandate is to ensure that all Laws, Policies, Programmes, and Administrative Mechanisms are in consonance with the Child Rights perspective as enshrined in the Constitution of India and also the UN Convention on the Rights of the Child.

****

Cyber Crimes against Women - 2020

SL	State/UT	Cyber Blackmailing/ Threatening (Sec.506, 503, 384 IPC r/w IT Act)	Cyber Pornography/ Hosting/ Publishing Obscene Sexual Materials (Sec.67A/67B(Girl Child) of IT act r/w other IPC/SLL)	Cyber Stalking/ Cyber Bullying of Women (Sec.354D IPC r/w IT Act)	Defamation/ Morphing (Sec.469 IPC r/w IPC and Indecent Rep. of Women (P) Act & IT Act)	Fake Profile (IT Act r/w IPC/SLL)	Other Crimes against Women	Total Cyber Crimes against Women
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
STATES:								
1	Andhra Pradesh	5	21	145	1	22	181	375
2	Arunachal Pradesh	0	0	0	0	0	1	1
3	Assam	2	211	1	0	182	675	1071
4	Bihar	0	3	11	2	4	27	47
5	Chhattisgarh	0	34	2	0	2	79	117
6	Goa	0	1	1	0	0	17	19
7	Gujarat	7	17	26	1	2	224	277
8	Haryana	1	64	19	1	16	121	222
9	Himachal Pradesh	0	31	7	0	7	7	52
10	Jharkhand	0	3	0	0	0	17	20
11	Karnataka	0	142	1	0	1	2715	2859
12	Kerala	0	113	14	1	5	113	246
13	Madhya Pradesh	6	52	28	2	2	184	274
14	Maharashtra	12	75	388	0	15	1142	1632
15	Manipur	0	3	3	0	0	20	26
16	Meghalaya	1	7	0	1	0	30	39
17	Mizoram	0	1	0	0	0	0	1
18	Nagaland	0	0	0	0	0	2	2
19	Odisha	1	292	0	220	13	34	560
20	Punjab	1	22	14	0	18	55	110
21	Rajasthan	3	24	12	1	3	195	238
22	Sikkim	0	0	0	0	0	0	0
23	Tamil Nadu	7	147	7	17	17	111	306
24	Telangana	19	11	100	1	14	504	649
25	Tripura	0	2	0	0	1	0	3
26	Uttar Pradesh	0	325	76	0	13	335	749
27	Uttarakhand	0	23	1	0	4	44	72
28	West Bengal	6	10	17	1	7	303	344
	TOTAL STATE(S)	**71**	**1634**	**873**	**249**	**348**	**7136**	**10311**
UNION TERRITORIES:								
29	A&N Islands	0	1	1	0	0	1	3
30	Chandigarh	0	1	1	0	0	8	10
31	D&N Haveli and Daman & Diu	0	0	0	0	0	3	3
32	Delhi	0	8	12	0	5	26	51
33	Jammu & Kashmir	3	10	0	2	1	9	25
34	Ladakh	0	0	0	0	0	0	0
35	Lakshadweep	0	1	0	0	0	1	2
36	Puducherry	0	0	0	0	0	0	0
	TOTAL UT(S)	**3**	**21**	**14**	**2**	**6**	**48**	**94**
	TOTAL ALL INDIA	**74**	**1655**	**887**	**251**	**354**	**7184**	**10405**

● As per data provided by States/UTs

● States/UTs may not be compared purely on the basis of crime figures

TABLE 9A.10 Page 1 of 1

Cyber Crimes against Children - 2020

SL	State/UT	Cyber Blackmailing / Threatening/ Harassment (Sec.506,503, 384 IPC r/w IT Act	Fake Profile (IT Act r/w IPC/SLL)	Cyber Pornography/ Hosting or Publishing Obscene Sexual Materials depicting children (Sec.67B of IT Act r/w other IPC/SLL)	Cyber Stalking/ Bullying (Sec.354D IPC r/w IT Act)	Internet Crimes through Online Games etc (Sec.305 IPC r/w IT Act)	Other Cyber Crimes against Children	Total Cyber crimes against Children
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
STATES:								
1	Andhra Pradesh	1	0	15	32	0	4	52
2	Arunachal Pradesh	0	0	0	0	0	0	0
3	Assam	0	0	21	0	0	24	45
4	Bihar	0	0	1	0	0	0	1
5	Chhattisgarh	0	1	3	3	0	14	21
6	Goa	0	0	0	0	0	3	3
7	Gujarat	0	0	1	4	0	27	32
8	Haryana	0	0	16	2	0	15	33
9	Himachal Pradesh	0	0	17	0	0	2	19
10	Jharkhand	0	0	0	0	0	4	4
11	Karnataka	0	0	122	0	0	22	144
12	Kerala	0	0	101	3	0	22	126
13	Madhya Pradesh	0	0	20	6	0	13	39
14	Maharashtra	1	0	123	69	0	14	207
15	Manipur	0	0	3	0	0	0	3
16	Meghalaya	0	0	0	0	0	0	0
17	Mizoram	0	0	0	0	0	0	0
18	Nagaland	0	0	0	0	0	0	0
19	Odisha	0	0	71	0	0	0	71
20	Punjab	0	0	8	0	0	2	10
21	Rajasthan	0	0	6	1	0	17	24
22	Sikkim	0	0	0	0	0	0	0
23	Tamil Nadu	0	0	28	0	0	7	35
24	Telangana	1	0	7	1	0	0	9
25	Tripura	0	0	0	0	0	0	0
26	Uttar Pradesh	0	0	161	14	0	22	197
27	Uttarakhand	0	0	11	0	0	0	11
28	West Bengal	0	0	0	2	0	4	6
	TOTAL STATE(S)	**3**	**1**	**735**	**137**	**0**	**216**	**1092**
UNION TERRITORIES:								
29	A&N Islands	0	0	1	0	0	0	1
30	Chandigarh	0	0	1	0	0	2	3
31	D&N Haveli and Daman & Diu	0	0	0	0	0	0	0
32	Delhi	0	0	1	3	0	1	5
33	Jammu & Kashmir	0	0	0	0	0	1	1
34	Ladakh	0	0	0	0	0	0	0
35	Lakshadweep	0	0	0	0	0	0	0
36	Puducherry	0	0	0	0	0	0	0
	TOTAL UT(S)	**0**	**0**	**3**	**3**	**0**	**4**	**10**
	TOTAL ALL INDIA	**3**	**1**	**738**	**140**	**0**	**220**	**1102**

● As per data provided by States/UTs

●States/UTs may not be compared purely on the basis of crime figures

TABLE 9A.11 Page 1 of 1