GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION No. 98
TO BE ANSWERED ON 7.12.2022

CYBER CRIME AGAINST WOMEN

98. DR. SUJAY RADHAKRISHNA VIKHE PATIL:
PROF. RITA BAHUGUNA JOSHI:
DR. HEENA GAVIT:
DR. KRISHNA PAL SINGH YADAV:
SHRI UNMESH BHAIYYASAHEB PATIL:
DR. SHRIKANT EKNATH SHINDE:

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

(a) whether the Government proposes a plan to deal with the cybercrime against women and hacking of their social media, if so, the details thereof;
(b) whether the Government has any action plan/ proposes to formulate a policy in order to address the hacking of social media platforms especially of women;
(c) if so, the details thereof; and
(d) the details of the number of cases reported by the cyber-crime branch with respect to social media hacking during the last three years and the current year?

ANSWER

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

(a) to (c): The Information Technology Act, 2000 ("IT Act") and rules made thereunder contain several provisions for safeguarding users in the cyberspace. The IT Act penalises 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. These cybercrimes are in addition to various cognizable offences punishable under the Indian Penal Code, 1860, such as the cognizable offence of stalking using electronic communication (section 354D). As per the provisions of the Code of Criminal Procedure, 1973, prevention and investigation of cognizable offences is to be done by the police. As per the Seventh Schedule to the Constitution, 'Police' is a State subject and, as such, States are primarily responsible for the prevention, investigation etc. of such cybercrimes through the State police departments, which take preventive and penal action as per law, including in respect of cybercrimes against women and hacking of their social media accounts.

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:

(i) To publish on their website and app, their rules and regulations, privacy policy and user agreement;

(ii) 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, among others, information which belongs to another person, or is obscene, or is invasive of another's privacy, or is insulting or harassing on the basis of gender, or is racially or ethnically objectionable, or encourages money laundering, or promotes enmity between different groups on the grounds of religion or caste with the intent to incite violence, or is harmful to child, or infringes intellectual property rights, or impersonates another person, or threatens the unity, integrity, defence, security or sovereignty of India or public order, or prevents investigation, or violates any law;

(iii) Upon receipt of an order from a lawfully authorised government agency, to provide information or assistance for prevention, detection, investigation or prosecution under law, or for cyber security incidents;

(iv) To have in place a grievance redressal machinery, and resolve complaints of violation of the rules within 72 hours of being reported;

(v) In case an intermediary is a significant social media intermediary (*i.e.,* an intermediary having more than 50 lakh registered users in India), to additionally observe due diligence in terms of appointing a Chief Compliance Officer, a nodal contact person for 24x7 coordination with law enforcement agencies and a Resident Grievance Officer, publishing monthly compliance reports, etc.

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.

In addition, the Ministry of Home Affairs operates a National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable citizens to report complaints pertaining to all types of cybercrimes, with special focus on cybercrimes against women.

The Ministry of Electronics and Information Technology is also implementing the Information Security Education and Awareness (ISEA) Phase-II project to build capacities in the area of information security, train government personnel and create mass information security awareness for various users. Under this, a large number of awareness workshops have been conducted across the country, school teachers trained as master trainers to reach out to crores of users in the indirect mode through Cyber Safety and Cyber Security Awareness Weeks organised in select cities in collaboration with State Cyber Cell / Police departments, mass awareness programmes broadcasted through Doordarshan / All India Radio, bimonthly newsletters published in print and digital mode, and multilingual awareness content in the form of handbooks, multimedia short videos, posters etc., which have been disseminated through print, electronic and social media and made available for download on the ISEA awareness portal (www.infosecawareness.in). A self-paced three module e-learning course on Cyber Hygiene Practices has also been made available on the portal, under which a large number of participants are registered and many have also obtained certification. The material designed and disseminated includes an exclusive handbook titled Information Security Awareness handbook for Women, and booklets on Cyber Security tips for Women and on Online Safety tips for Women@Home during COVID 19.

(d): Data on crime is maintained by the National Crime Records Bureau. As per the Bureau, no specific data with respect to social media hacking is available with it. The crime-head-wise data under the category of cybercrimes against women is at Annex.

******

Annexure

Crime-head-wise cases registered under the category cybercrimes against women

S. no.	Crime heads	2018	2019	2020	2021

1	Cyber blackmailing or threatening {sections 506, 503 and 384 of the Indian Penal Code, 1860 (IPC), read with the Information Technology Act, 2000 (IT Act)}	113	108	74	200
2	Cyber pornography or hosting or publishing obscene sexual materials {sections 67A or 67B (girl child) of the IT Act, read with other IPC or special and local laws (SLL)}	862	1,174	1,655	1,896
3	Cyber stalking or cyber bullying of women (section 354D of IPC), read with the IT Act	738	785	887	1,172
4	Defamation or morphing {section 469 of IPC, read with IPC and the Indecent Representation of Women (Prohibition) Act, 1986}	62	65	251	276
5	Fake profile (read with IPC/SLL)	207	288	354	225
6	Other crimes against women	4,048	5,995	7,184	6,961
	Total	**6,030**	**8,415**	**10,405**	**10,730**

Source: National Crime Records Bureau

******