GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1014
TO BE ANSWERED ON: 08.02.2023

IT POLICY AGAINST WEAPONIZED TECHNOLOGY

1014. SHRIMATI APARUPA PODDAR:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether the government intends to prepare draft for stringent IT policy against weaponised technology in the light of recent cases of breaches of online safety and national security hack and if so, the details thereof;
(b) whether the government plans to revise the rule for social media platforms under safe harbour principle and if so, the details thereof; and
(c) the action taken on the rising cases of commodification and harassment of women on social media platforms?

ANSWER

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

(a): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. With the expansion of the Internet and more and more Indians coming online, the possibility that Digital Nagrik or citizens being exposed to user harms, disinformation and criminality has also increased. Government is fully cognizant and aware of various cyber security threats, and has taken measures to mitigate citizens vulnerability to cyber-attacks.

The National Security Council Secretariat (NSCS) has formulated a draft National Cyber Security Strategy, which holistically looks at addressing the issues of security of national cyberspace.

(b):The Central Government, in exercise of powers conferred by the IT Act, has notified amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021("IT Rules, 2021"). These rules cast specific obligation on intermediaries vis-à-vis what kind of information is to be hosted, displayed, uploaded, published, transmitted, stored or shared. Intermediaries are also required to remove any content violative of any law for the time being in force as and when brought to their knowledge either through a court order or through a notice by appropriate government or its authorised agency. In case of failure to follow diligence as provided in the IT Rules, 2021, by intermediaries, they shall lose their exemption from liability under section 79 of the IT Act and shall be liable for consequential action as provided in such law. Such diligence includes the following:

(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 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, three Grievance Appellate Committee(s) have been constituted to enable users to appeal against decisions taken by Grievance Officers on such complaints.

(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 offences relating to computer resources, including identity theft (section 66C), violation of bodily privacy (section 66E), publishing or transmitting of obscene material in electronic form (section 67), and publishing or transmission of material containing sexually explicit act in electronic form (section 67A and 67B), etc. Each such offence 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 offences 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, and as per the Seventh Schedule to the Constitution, 'Police' is a State subject. 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.

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.

******