GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2408
TO BE ANSWERED ON: 21.12.2022

DEEP FAKE APP

2408. SHRI GANESH SINGH:

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

(a) whether the Government is aware that the Deepfake App has emerged as a new alternative to spread propaganda and rumours on a large scale;
(b) whether Deepfake App can inflict harm to any person, institution, businesses and even a democratic system in many ways and if so, the details thereof;
(c) whether criminals are using Deepfake app as a weapon to entrap women in most of the cases of pornography;
(d) whether the misuse of app like Deepfake may pose a danger to political and social stability and national security; and
(e) if so, the details thereof along with the action taken by the Government in this regard?

ANSWER

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

(a) to (e): The policies of the Government are aimed at ensuring an Open, Safe, Trusted and Accountable Internet for its users. With the expansion of the Internet and more and more Indians coming online, the potential for information that may be harmful or pornographic or threatens national security, or is misinformation orinformation that is patently false and untrue or misleading in nature, has grown. The Government is cognizant of new and evolving technologies, including technologies that alter the image or voice of a person to make it appear to be that of another person, or that create image or voice that appears to be that of a person, enabling creation of "deep fakes", may pose security risk to individuals, enterprises and the nation.

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 tampering with computer source documents (section 65), publishing or transmitting of obscene material in electronic form or containing sexually explicit act(sections 67, 67A and 67B), 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.

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.

To ensure that Internet in India is Open, Safe and Trusted and Accountable, 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, the amended Rules 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. For evolving technologies and their possible misuse, the Government also continuously interacts with the stakeholders including identification of possible legislative changes.

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.

******