

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION No. 3447
TO BE ANSWERED ON 31.3.2023

DEEPFAKES

3447. SHRI JAWHAR SIRCAR:

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

- (a) Government's plan to take Artificial intelligence created deepfakes that deceive people by making someone appear to say or do something they did not do or say.;
- (b) whether Government is satisfied with the tools designed to detect manipulated content capable of deep fakes or would Government seek to cooperate with proven fact-checkers; and
- (c) whether Government is examining the new regulations issued by other countries like China's cyberspace administration's order of January 10, that aims to protect people from uninvited impersonation using "Deep Synthesis Technology"?

ANSWER

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

(a) to (c): 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 "deepfakes".

The Information Technology Act, 2000 ("IT Act") and rules made thereunder contain several provisions for safeguarding users in the cyberspace. To ensure that Internet in India is Open, Safe and Trusted and Accountable, the Central Government, while taking into account international developments in social media regulation, in exercise of powers conferred by the IT Act, has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021"). These rules cast specific obligation on intermediaries, including social media intermediaries, to observe due diligence and provide that if they fail to observe such due diligence, they shall no longer be exempt from their liability under law for third-party information or data or communication link hosted by them. The said Act and rules provide for the following:

- (i) Sub-clause (vi) of clause (b) of sub-rule (1) of rule 3 provides that an intermediary including a social media intermediary shall observe due diligence while discharging its duties by making reasonable efforts to cause the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that impersonates another person.
- (ii) Section 66D of the IT Act provides that whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment and be liable to fine, and in terms of the provisions of section 77B, the same is a cognizable offence. This is in addition to various cognizable offences punishable under the Indian Penal Code, 1860, which may also be attracted in instances of criminal use of deepfakes. 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.
- (iii) Clause (d) of sub-rule (1) of rule 3 provides that an intermediary on whose computer resource information prohibited under any law for the time being in force is stored,

hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its authorised agency, shall not host, store or publish such information, and shall remove the unlawful information or disable access thereto within 36 hours from receipt of the court order or being notified.

- (iv) Rule 3(2)(b) provides that the intermediary shall, within 24 hours from receipt of a complaint made by an individual or any person on his behalf, in relation to any content which is *prima facie* in the nature of impersonation in electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.
- (v) Clause (c) of sub-rule (1) of rule 3 also provides that the intermediary shall periodically inform its users, at least once every year, that in case of non-compliance with its rules and regulations or user agreement, it has the right to terminate the access or usage rights of the users immediately or remove non-compliant information.

The Ministry of Electronics and Information Technology has issued an advisory on 21.2.2023 to significant social media intermediaries, drawing their attention to the above provisions and advising them as under:

- (i) That they should ensure that their rules and regulations and the user agreement contain appropriate provisions for the users not to host, display, upload, modify, publish, transmit, store, update or share any information that impersonates another person, and that the users are duly informed of the same;
- (ii) That, as part of the reasonable efforts made by them in this regard, they may also put in place appropriate technology and processes for identifying information that may violate the provisions of rules and regulations or user agreement; and
- (iii) That they are advised to ensure expeditious action, well within the timeframes stipulated under the IT Rules, 2021, to remove or disable access to information/content that violates the aforesaid provisions of the IT Rules, 2021, upon receipt of court orders or notification from the Appropriate Government or its authorised agency or on complaint made by the impersonated individual or person authorised by him in this behalf.

Government has also established Grievance Appellate Committees to allow users and victims to appeal online on www.gac.gov.in against decisions taken by the Grievance Officers of intermediaries in case they are dissatisfied with the decision of the Grievance Officer. 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, and also operates a toll-free helpline (1930).
