

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 728
TO BE ANSWERED ON: 08.12.2023

THREATS AND DANGERS OF ARTIFICIAL INTELLIGENCE

728. SHRI PARIMAL NATHWANI:

Will the MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) the prevalent threats and dangers of Artificial Intelligence (AI) in India;
- (b) the legal safeguards in vogue against misuse of AI in the country;
- (c) the safeguards against use of fake and deep fakes using IT tools; and
- (d) the steps contemplated by Government so that AI doesn't become a menace?

ANSWER

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

(a) to (e): Government of India expects artificial intelligence to be an enabler of India's fast growing digital and innovation economy. The Government wants AI to be used with safety and trust for all users. The concerns and risks associated with AI have been highlighted in the National Strategy for AI (NSAI) released in June, 2018. Various central and state government departments and agencies have commenced efforts to standardize responsible AI development, use and promote the adoption of best practices. Additionally, NITI Aayog has published a series of papers on the subject of Responsible AI for All. Further, as a founding member and council chair of the Global Partnership on Artificial Intelligence (GPAI), India assumes a leading role in guiding the responsible development and use of AI. The Information Technology Act, 2000 ("IT Act") and rules made thereunder contain several provisions for safeguarding users from harms emanating through use of information technology including artificial intelligence (AI). The IT Act penalizes various offences relating to computer resources, including tampering with computer source documents (section 65), dishonestly or fraudulently damaging computer system (section 66), identity theft (section 66C), cheating by impersonation (section 66D), etc. In addition to such general provisions regarding cyber offences, it also provides for various offences that serve to secure the digital space for women, e.g., 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). Further, the new IT 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. Further, in case an intermediary is a significant social media intermediary (an intermediary having more than 50 lakh registered users in India), it shall additionally observe due diligence in terms of appointing, in India, a Grievance Officer, a Chief Compliance Officer and a nodal contact person for 24x7 coordination with law enforcement agencies. As per the IT Rules, 2021, the Chief Compliance Officer is responsible for ensuring compliance with the IT Act and the rules made thereunder. Keeping in view complaints about the intermediary's action or inaction on objectionable content or suspension of accounts, the Central Government has also established three GACs (Grievance Appellate Committees) to enable users to appeal against the decisions taken by Grievance Officer of intermediaries on user complaints.
