GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *51
TO BE ANSWERED ON: 29.11.2024

INDIVIDUAL PRIVACY AND DATA SECURITY AMIDST AI

***51. SHRI VIVEK K. TANKHA:**

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

(a) the steps taken by Government to ensure individual privacy and data security amidst rapid growth of Artificial Intelligence (AI);

(b) statistics on AI related data breaches or misuse of personal information in the country including reported cases of AI enabled cyber fraud in the past five years; and

(c) the details of initiatives taken by Government to promote transparency and accountability in AI algorithms, and steps taken to reduce AI-enabled cyber fraud?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (c): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *51 FOR 29.11.2024 REGARDING INDIVIDUAL PRIVACY AND DATA SECURITY AMIDST AI

(a) to (c): The policies of Government of India are aimed at ensuring an open, safe, trusted and accountable cyberspace for users in the country amidst AI growth. Among the key steps taken by Government of India to ensure individual privacy and data security in cyber space are Information Technology Act, 2000 ("IT Act") and Digital Personal Data Protection Act, 2023 ("DPDP Act"). These Acts regulate the information that is generated using Artificial Intelligence ("AI") tools or any other technology and those which are generated by users themselves ensuring individual privacy and data security.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021")under IT Act cast specific due diligence obligations on intermediaries with respect to the information that is not to be hosted, displayed, uploaded, published, transmitted, stored or shared on the platforms. Intermediaries are required not to host, store or publish any information violative of any law for the time being in force. In case of failure to observe due diligence as provided in the IT Rules, 2021, intermediaries lose the exemption from liability for any third-party information, data or communication link, under section 79 of the IT Act.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 under IT Act has prescribed reasonable security practices and procedures and sensitive personal data or information to protect sensitive personal data of users. These include the requirement that any person collecting, receiving, possessing, storing or dealing information should publish on its website a privacy policyand disclosure of personal information, that such person use the information collected for the purpose for which it was collected and keep it secure, that disclosure of sensitive personal data be done with prior permission of the information provider, that sensitive personal data or information not be published, and that a third party receiving sensitive personal data or information shall not disclose it further. Also, Section 72A of the Act provides for punishment for disclosure of information in breach of the lawful contract.

The DPDP Act provides for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes. The DPDP Act provides a comprehensive framework for the protection of digital personal data of the individuals and ensures its security while making data fiduciaries accountable for personal data breaches. The Act mandates data fiduciaries to adopt reasonable security safeguards and adopt technical and organizational measures to comply with the provisions of the Act.

Under the approved IndiaAI Mission - "Safe & Trusted AI" Pillar, IndiaAI has selected eight Responsible AI Projects against the Expression of Interest (EoI). These projects address the need for robust guardrails to ensure the responsible development, deployment, and adoption of AI technologies. The selected projects focus on developing indigenous tools and frameworks and establishing guidelines for ethical, transparent, and trustworthy AI. The projects cover a range of critical themes, including Machine Unlearning, Synthetic Data Generation, AI Bias Mitigation, Ethical AI Frameworks, Privacy-Enhancing Tools, Explainable AI, AI Governance Testing, and Algorithm Auditing Tools.

With regard to the AI-related data breaches or misuse of personal information, as per National Crime Record Bureau, there is no information available with them.

Further, to address the emerging harms in the cyberspace like misinformation, deepfakes powered by AI, Ministry of Electronics and Information Technology conducted multiple consultations with industry stakeholders/ social media platforms and issued an advisory dated 26.12.2023 and subsequently issued another advisory on 15.03.2024, through which the intermediaries were reminded about their due-diligence obligations outlined IT Rules, 2021 and advised on countering unlawful content including malicious 'synthetic media' and 'deepfakes'.

The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis. In this context, an advisory on safety

measures to be taken to minimize the adversarial threats arising from Artificial Intelligence (AI) based applications was published in May 2023.

****