GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**RAJYA SABHA**
**UNSTARRED QUESTION. NO. 2463**
TO BE ANSWERED ON: 21.03.2025

## SAFEGUARDING PRIVACY AND ADDRESSING BIAS IN AI APPLICATIONS

**2463. SHRI SUJEET KUMAR:**

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

(a) the measures being implemented by the Ministry to protect citizens' privacy in the collection, storage, and use of data for Artificial Intelligence (AI) applications;
(b) whether the Ministry is taking steps to address concerns regarding potential biases in AI algorithms, particularly in decision-making processes that may impact individuals' lives;
(c) if so, the details thereof, including any guidelines, regulations or frameworks established to ensure fairness and accountability in AI systems; and
(d) if not, the reasons therefor and whether Government plans to introduce any initiatives in this regard?

**ANSWER**

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): Government is committed to harnessing the power of Artificial Intelligence (AI) for the good of our people in sectors like healthcare, agriculture and education while mitigating risks associated with AI deployment. The Government has constituted an Advisory Group on AI for India-specific regulatory AI framework with an objective to address issues related to development of Responsible AI framework for safe and trusted development and deployment of AI.

Among the key steps taken by the Government of India to ensure individual privacy and data security in cyber space are the Information Technology Act, 2000 (“IT Act”) and Digital Personal Data Protection Act, 2023 (“DPDP Act”). These Acts regulate the information that is generated using AI tools or any other technology and those which are generated by users themselves ensuring individual privacy and data security. 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.

The report on AI Governance Guidelines Development emphasizes the need for a coordinated, whole-of-government approach to ensure effective compliance and enforcement as India’s AI landscape continues to evolve. Given the evolving nature of AI technologies, the report recommends adoption of a techno legal approach to AI regulation. Public consultation on the report on AI Governance Guidelines Development has been completed. Under the IndiaAI Mission - “Safe & Trusted AI” Pillar, IndiaAI has selected eight Responsible AI Projects. 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.
Moreover, 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.

Further, to address the emerging harms in the cyberspace like misinformation, deepfakes, Government had multiple consultations with industry stakeholders/ social media platforms and advisories were issued, where in the intermediaries were reminded about their due-diligence obligations outlined under 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 issued.

*******