LIABILITIES ARISING FROM AI USAGE

3090. SHRI ANURAG SINGH THAKUR:

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

(a) the definition of Artificial Intelligence (AI) that has been adopted in the recently issued AI Governance Guidelines, particularly given observations that "AI" is largely a marketing term for advanced machine learning applications;
(b) the manner in which the Ministry plans to balance promoting innovation with mitigating risks specifically;
(c) the manner in which it intends to differentiate and regulate high-risk versus low-risk machine learning applications in sectors such as healthcare and aviation;
(d) whether liabilities arising from AI usage will be primarily managed through contractual agreements or require new state interventions and if so, the details thereof; and
(e) the manner in which existing digital technology laws and governance frameworks are likely to be integrated with the new guidelines to ensure responsible, accountable and economically enabling AI development in the country?

ANSWER

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

(a) to(e): The Government of India emphasizes the concept of 'AI for All,' aligning with the Hon'ble Prime Minister's vision to democratise use of technology. This initiative aims to ensure that AI benefits all sectors of society, driving innovation and growth.

Government is committed to harnessing the power of Artificial Intelligence (AI) for the good of our people in sectors like healthcare, agriculture and education. At the same time, the Government is cognizant of the risks posed by AI and the need to create guardrails to ensure that AI issafe and trusted.

Government has constituted an **Advisory Group on AI for India-specific regulatory AI framework** under the chairmanship of Principal Scientific Advisor (PSA) to Hon'ble Prime Minister of India with diverse stakeholders from academia, industry and government with an objective to address all issues related to development of Responsible AI framework for safe and trusted development and deployment of AI. 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. The report acknowledge that the term "Artificial Intelligence" (AI) has been widely used in industry and policy discourse, often encompassing a broad range of computational techniques. While commonly associated with advanced machine learning applications, the report emphasises that AI should be defined in a way that reflects both its technological capabilities and socio-economic implications.Recognising AI as a rapidly evolving field, the report highlights the importance of keeping the **definition adaptable to future advancements**. Public consultation on the report on AI Governance Guidelines Development has been completed and more than 100 suggestions have been received.

In addition, the Government has taken several steps to mitigate the risks from misuse of AI enabled technologies like Deepfakes & AI generated content to spread misinformation. The Government has notified the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021")** on 25.02.2021 which was subsequently amended 28.10.2022 and 6.4.2023. The IT Rules, 2021 cast specific legalobligations on intermediaries, including social media intermediaries and platforms, to ensuretheir accountability towards safe and trusted internet including their expeditious action towards removal of the prohibited misinformation, patently false information and deepfakes. In case of failure of the intermediaries to observe the legal obligations as provided in the ITRules, 2021, they lose their **safe harbour protection under section 79 of the Information Technology Act, 2000 ("IT Act")** and shall be liable for consequential action or prosecution as provided under any extant law.

Also, the **Digital Personal Data Protection Act, 2023** has been enacted on 11th August, 2023 whichcasts obligations on Data Fiduciaries to safeguard digital personal data, holding them accountable, while also ensuring the rights and duties of Data Principals.

Union Cabinet led by Hon'ble Prime Minister has approved the IndiaAI Mission on 7th March 2024, a strategic initiative to establish a robust and inclusive AI ecosystem that aligns with the country's development goals. This mission is driven by a vision to position India as a global leader in artificial intelligence by focusing on seven foundational pillars: IndiaAI Compute, IndiaAI FutureSkills, IndiaAI Startup Financing, IndiaAI Innovation Centre, IndiaAI Datasets Platform, IndiaAI Applications Development Initiative and Safe & Trusted AI.

The 'Safe & Trusted' pillar within the IndiaAI Mission aims to encourage the adoption of AI in a responsible manner with the principles of safety, security, transparency, and privacy embedded in the design of AI technology to mitigate the AI risks, placing the idea of 'AI for All' at its very core.This pillar enables the implementation of Responsible AI projects including the development of indigenous tools and frameworks, self-assessment checklists for innovators, and other guidelines and governance frameworks.

Eight Responsible AI Projects have been selected to address the need for robust guardrails to ensure the responsible development, deployment, and adoption of AI technologies. 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.The details of the selected projects are given at Appendix I.

****

The details of the selected projects under "Safe & Trusted AI" Pillar are as under:

NAME OF THE THEME	SELECTED APPLICANT	TITLE OF THE PROJECT
Machine Unlearning	IIT Jodhpur	Machine Unlearning in Generative Foundation Models
Synthetic Data Generation	IIT Roorkee	Design and Development of Method for Generating Synthetic Data for Mitigating Bias in Datasets; and Framework for Mitigating Bias in Machine Learning Pipeline for Responsible AI
AI Bias Mitigation Strategy	National Institute of Technology Raipur	Development of Responsible Artificial Intelligence for Bias Mitigation in Health Care Systems
Explainable AI Framework	DIAT Pune and Mindgraph Technology Pvt. Ltd.	Enabling Explainable and Privacy Preserving AI for Security
Privacy Enhancing Strategy	IIT Delhi, IIIT Delhi, IIT Dharwad and Telecommunication Engineering Center (TEC)	Robust Privacy-Preserving Machine Learning Models
AI Ethical Certification Framework	IIIT Delhi and Telecommunication Engineering Center (TEC)	Tools for assessing fairness of AI model
AI Algorithm Auditing Tool	Civic Data Labs	ParakhAI - An open-source framework and toolkit for Participatory Algorithmic Auditing
AI Governance Testing Framework	Amrita Vishwa Vidyapeetham and Telecommunication Engineering Center (TEC)	Track-LLM, Transparency, Risk Assessment, Context & Knowledge for Large Language Models

******