GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 3130
TO BE ANSWERED ON: 19.03.2025

ARTIFICIAL INTELLIGENCE REGULATORY FRAMEWORK

3130. SHRI KRISHNA PRASAD TENNETI:

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

(a) the measures being undertaken by the Government to formulate a regulatory framework for Artificial Intelligence (AI) technologies considering its ethical and economic impacts;
(b) the measures being taken by the Government to ensure that India's approach towards AI is independent and protects the sovereignty of the country in view of the cross-border nature of AI technologies;
(c) the details and the number of cases reported, chargesheets drawn and convictions made regarding deepfakes and other unethical practices facilitated by AI during the last three years, State-wise especially in Andhra Pradesh; and
(d) the steps being taken by the Government to protect the citizens from the adverse effects of AI along with details of the present governance framework for AI?

ANSWER

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

(a) to (d): 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.

The policies of the Government are aimed at ensuring an open, safe, trusted and accountable internet for users in the country amidst AI growth.

The Government is committed to harnessing the power of Artificial Intelligence (AI) for the good of our people in sectors like healthcare, agriculture, education, Governanceand others. At the same time, the Government is cognizant of the risks posed by AI like Hallucination, bias, misinformation and deepfakes are some of the challenges posed by AI.

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.Public consultation on the report on AI Governance Guidelines Development has been completed and more than 100 suggestions have been received.

To address the challenges and risks of AI the **Government is cognizant of the need to create guardrails to ensure that AI is safe and trusted**. Accordingly, the Central Government after extensive public consultations with relevant stakeholders 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 legal obligations on intermediaries, including social media intermediaries and platforms, to ensure their 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 IT Rules, 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.

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

India as a founding member and current council chair of the Global Partnership on Artificial Intelligence (GPAI) has organized the Global IndiaAI Summit and GPAI Summit in July 2024 and December 2023 where various stakeholders from government, industry and academia engaged in discussions and deliberations for development of AI based solutions in a safe and trusted manner. India has taken lead in ensuring that AI is available for all and for developing global framework for safety & trust for AI models and applications.

With regard to the cases reported, chargesheets drawn and convictions made regarding deepfakes and other unethical practices, there is no information available with this ministry.

The Government has taken various steps to protect the citizens from the adverse effects as follows:

i) 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.

ii) CERT-In conducts joint cyber security training programs in collaboration with Industry partners to upskill the cyber security workforce in Government, public and private organizations with the latest skills. Technical training sessions in the area of AI-powered cybersecurity threats were conducted with experts from Industry to help the participants understand the latest threat landscape and best practices.

iii) The Certified Security Professional in Artificial Intelligence (CSPAI) program launched by CERT-In and SISA in September 2024. The certification is approved by the ANSI National Accreditation Board (ANAB) by meeting the ISO/IEC 17024 standard. The program aims to address the growing need for Secure and Responsible AI integration into business applications and processes. The CSPAI program equips cybersecurity professionals with the skills to secure AI systems, proactively address AI-related threats, and ensure trustworthy AI deployment in business environments.

iv) CERT-In is one of the International partners to co-sign the joint high-level risk analysis report on Artificial Intelligence (AI) entitled "Building trust in AI through a cyber-risk-based approach," published by the National Cybersecurity Agency for France (ANSSI) in February 2025. The report advocates for a risk-based approach to support trusted AI systems and secure AI value chains and calls for discussions on AI-related cyber risks and how to mitigate them to foster trusted AI development.

v) CERT-In has published a whitepaper in August 2023, highlighting the increasing attacks on Application Programming Interface (API) and how AI can be useful in mitigating these attacks.

vi) CERT-In published "Cyber Security Guidelines for Smart City Infrastructure" in February 2025 including measures for secure usage of Artificial Intelligence (AI) and Machine Learning (ML) for smart city infrastructure and applications.

****