

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1805
TO BE ANSWERED ON: 29.07.2026

**COLLECTION AND USE OF PERSONAL DATA BY FOREIGN DIGITAL/
TECHNOLOGIES COMPANIES**

†1805. SHRI AMRA RAM:

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

- (a) whether the foreign digital/technology companies are collecting and using the personal data of Indian citizens on a large scale;
- (b) if so, the steps taken by the Government to ensure the security of such data, data storage in the country and the privacy of citizens;
- (c) whether the Government proposes to introduce any new policy or regulatory framework to ensure the accountability of foreign digital companies and compliance with Indian laws; and
- (d) if so, the details thereof and if not, the reasons therefor?

ANSWER

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

(a) to (d): The policies of Government of India are aimed at ensuring an open, safe, trusted and accountable cyberspace for users in the country. Government of India has taken major initiatives like enactment of Information Technology Act, 2000 (IT Act), setting up of Indian Computer Emergency Response Team (CERT-In), releasing of National Cyber Security Policy 2013 and enactment of Digital Personal Data Protection Act 2023 (DPDP Act), thus ensuring security and protecting privacy of users in India.

Information Technology Act, 2000 (IT Act):

- (i) The Information Technology (IT) Act, 2000 provides a technology-neutral legal framework governing electronic transactions, protection of computer resources, cybersecurity, intermediary due diligence and cyber offences.
- (ii) The Act applies to entities providing digital services in India, irrespective of their place of incorporation. Further, under Section 75 of the IT Act, its provisions have extra-territorial application to offences or contraventions committed outside India where the act or conduct involves a computer, computer system or computer network located in India.
- (iii) The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 prescribe due diligence obligations for intermediaries, including significant social media intermediaries, with a view to promoting a safe, trusted and accountable online environment.

(iv) The due diligence framework under the IT Rules, 2021 requires intermediaries to, inter alia, exercise due diligence in discharging their duties, take reasonable steps to prevent the hosting or dissemination of unlawful information, provide grievance redressal mechanisms, and comply with lawful directions issued by competent authorities in accordance with the provisions of the IT Act and the Rules.

(v) Moreover, the Government has prescribed stringent security requirements for the empaneled cloud service providers who are handling government data including compliance with international security and privacy standards along with other security requirements to ensure cloud security, service management, and data protection. These compliances and standards cover critical security aspects such as risk assessment, security controls, service delivery, incident management, intrusion detection, data privacy, log retention, data encryption, access control, etc.

Digital Personal Data Protection Act 2023 (DPDP Act):

(i) DPDP Act, 2023 provides a comprehensive legal framework for processing digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such data for lawful purposes.

(ii) To operationalise the Act, the Digital Personal Data Protection Rules, 2025 were notified on 13 November 2025. The provisions of the Act and the Rules are being implemented in a phased manner.

(iii) The Act permits the processing of personal data for lawful purposes either on the basis of the consent of the Data Principal or for certain legitimate uses specified under the Act.

(iv) Where processing is based on consent, such consent must be free, specific, informed, unconditional and unambiguous, and must be preceded or accompanied by a notice specifying the personal data to be processed and the purpose of such processing.

(v) The Act places obligations on Data Fiduciaries (entities that determine the purpose and means of processing personal data) to:

- implement reasonable security safeguards to protect personal data;
- establish effective grievance redressal mechanisms; and
- notify the Data Protection Board of India and affected Data Principals in the event of a personal data breach.

(vi) The Data Protection Board of India is empowered to inquire into personal data breaches and other contraventions of the Act and impose monetary penalties in accordance with its provisions.

(vii) The Act applies to the processing of digital personal data within India and also to processing outside India where such processing is undertaken in connection with offering goods or services to Data Principals in India. Accordingly, its provisions extend to foreign digital and technology companies engaged in such processing.

(viii) The Act also empowers the Central Government to notify restrictions on the transfer of personal data to such countries or territories outside India as may be considered necessary.

Public Awareness Activities:

(i) The Government is implementing the Information Security Education and Awareness (ISEA) project to build human resources in information security and promote awareness on cyber hygiene and cyber security among citizens.

(ii) Under the ISEA project, over 6,650 awareness workshops have been conducted across the country, covering more than 11.37 lakh participants, including school and college students, teachers, law enforcement personnel, government officials and the general public.

(iii) Multilingual awareness material, including handbooks, short videos, posters, brochures and cartoon stories for children, has been developed and disseminated through print, electronic and social media, as well as through the ISEA and Stay Safe Online portals i.e. www.isea.gov.in & <https://staysafeonline.in/>.

(iv) The Government also organises nationwide awareness campaigns such as Cyber Security Awareness Month and Safer Internet Day to promote safe online behaviour, secure digital transactions and responsible use of digital services.

(v) Cyber security advisories are issued regularly on emerging cyber threats, mitigation strategies and best practices. Initiatives such as the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) and the National Cyber Coordination Centre (NCCC) strengthen cyber resilience by detecting and mitigating malicious activities and enhancing situational awareness.

(vi) Indian Computer Emergency Response Team (CERT-In) regularly disseminates cyber safety and security advisories, awareness posters, infographics and videos through its official website and social media platforms to sensitise internet users about cyber threats, online frauds and safe online practices, including online safety measures for children.

(vii) The Ministry of Education issued the PRAGYATA Guidelines on Digital Education in July 2020, providing a framework for safe and effective online learning, including the promotion of students' well-being and responsible use of social media and digital devices.

(viii) The Central Board of Secondary Education (CBSE) has supplemented these efforts by issuing guidelines on digital etiquette, conducting cyber security training for teachers, publishing the Cyber Security Handbook, and advising schools to establish Cyber Clubs to promote cyber safety awareness.

(ix) The National Council of Educational Research and Training (NCERT) has integrated cyber safety into the school curriculum, including a chapter on "Societal Impacts" for Classes XI and XII. In addition, CIET-NCERT has developed and disseminated educational resource materials on cyber safety.
