GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 5327
TO BE ANSWERED ON 25.03.2026

USE OF TECHNOLOGY FOR ESPIONAGE

5327. SHRI RAHUL GANDHI:

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

(a) whether the Government is aware of the growing use of technology — including mobile phones and cameras — for espionage;
(b) the reasons for the delay in addressing CCTV security vulnerabilities despite informing Parliament in 2021 that 10 lakh Chinese-origin cameras were in use by the Government and posed data transfer risks;
(c) the total number of CCTV cameras procured during the last five years, by country of origin, proportion certified as not being vulnerable and standards used for such certification;
(d) whether the Government is aware that Chinese mobile applications banned for data transfer risks continue operating in the country under rebranded versions and if so, the list of such applications along with action taken thereon;
(e) the details of security protocols governing AI systems used by the Government including foreign AI platforms currently in use; and
(f) the measures undertaken to protect India's data security and digital sovereignty from cyber threats and foreign surveillance?

ANSWER

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

(a) to (f): Government of India is conscious of the cybersecurity risks posed by digital technologies. In last 12 years, numerous efforts have been made to strengthen India's digital ecosystem, outlined below.

Protecting India's telecom networks:
Telecom networks are the most critical part of digital infrastructure. In 2021, Government undertook decisive step to implement National Security Directive on Trusted Sources. It ensures that telecommunication equipment only from the trusted sources is deployed in the telecom networks in the country.

Strengthening legal framework:
Government has strengthened the legal framework pertaining to network security and data protection. Government has notified the Telecommunication Act, 2023 containing extensive

provisions for security of telecommunication networks in the country and Digital Personal Data Protection Act, 2022 containing legal framework to ensure protection of personal data.

Strengthening security of CCTV systems:

Government has undertaken major reforms for strengthening of security of CCTV systems and notified the mandatory Essential Requirements required for CCTVs in Indian market.

Additional security requirements are as follows:

- For ensuring hardware security, clear documentation of the origin of critical components (like System-on-Chip or SoC) is now mandatory.
- Devices must be tested against vulnerabilities that could allow unauthorized remote access.
- Devices must now undergo testing at accredited labs.

At present, 507 models of CCTVs cameras are certified for compliance of ERs.

CCTV use by Governments:

Government departments have been restricted from buying CCTV equipment that does not meet these criteria.

Additionally, an advisory was issued to all Ministries for taking appropriate measures to address the security threats of the CCTV network vulnerability and to ensure the overall security and integrity of CCTV/Video Surveillance Systems.

Blocking mobile applications:

Government of India has blocked 652 mobile applications on account of concerns relating to data security and other malpractices under Section 69A of the IT Act, 2000.

Additional measures to enhance cybersecurity posture:

- National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.
- CERT-In has empanelled 237 security auditing organizations to support and audit implementation of Information Security Best Practices.
- CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.
- CERT-In has issued updated technical guidelines in July 2025 for Bill of Materials (BOM) for software, hardware, Artificial Intelligence, Quantum Computing & Cryptography requirements. These guidelines are aimed to enhance the security and transparency of supply chains for software, hardware & emerging technologies.

****