

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO.2651
TO BE ANSWERED ON: 25.03.2022

BAN ON CHINESE APPS

2651. SHRI SUSHIL KUMAR GUPTA:

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

- (a) whether it is a fact that Government has issued fresh orders to ban over 54 Chinese apps, terming them as a threat to privacy and security of Indians; and
- (b) if so, the other measure that are being taken to protect the privacy and security of Indians as far as IT is concerned?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): Yes, Sir. In line with the objective of the Government to ensure an Open, Safe & Trusted and Accountable Internet for all its users and based on the requests received through designated nodal officers from Ministry of Home Affairs (MHA), the Ministry of Electronics and Information Technology (MeitY) has blocked 54 mobile applications under the provision of section 69A of the Information Technology (IT) Act, 2000 and the Information Technology (Procedure and Safeguards for Blocking for Access of Information for Public) Rules, 2009. These mobile applications were blocked in the interest of sovereignty and integrity of India, defense of India and security of the State. As per the information made available by MHA, these apps were collecting various user data and transmitting it in an unauthorized manner to servers abroad for profiling.

(b): At present Section 43A and section 72A of the IT Act, 2000 enable privacy and security of sensitive personal data in digital form. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), Rules, 2011, provides reasonable security practices and procedures by the body corporate. In financial sector, RBI has mandated that all payment system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. For the foreign leg of the transaction, if any, data can also be stored in the foreign country, if required.

The Government has also introduced the Personal Data Protection Bill in Parliament in the year 2019 and the same was referred to Joint Committee of Parliament (JCP). Now the JCP has tabled

its report in December, 2021 in Parliament. The report and the Bill are under examination in MeitY.

Further, Government has taken following measures to enhance the cyber security posture and prevent cyber-attacks:

- i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. CERT-In has issued 68 advisories for organizations and users for data security and mitigating fraudulent activities.
- ii) Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.
- iii) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
- iv) CERT-In has empaneled 96 security auditing organizations to support and audit implementation of Information Security Best Practices.
- v) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organizations regarding securing the IT infrastructure and mitigating cyber-attacks. 15 and 19 training programs were conducted covering 708 and 5169 participants during the year 2020 and 2021 respectively.
- vi) CERT-In is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for citizens and organizations.
- vii) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.
- viii) MeitY is conducting programs to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security which are disseminated through portals like “www.infosecawareness.in”, and “www.cyberswachhtakendra.gov.in”.
