GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2007
TO BE ANSWERED ON 17.3.2023

LEAKAGES IN AADHAR DATABASE

2007. SMT. VANDANA CHAVAN:

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

(a) whether Government is aware of the recent breaches of security where Aadhaar is being leaked and sold along with other personal data of citizens;
(b) the number of recorded leakages of the Aadhaar database in the last five years;
(c) the various threats involved in such unauthorised access to the Aadhaar database; and
(d) the steps taken by Government to strengthen cyber security and prevent such breaches of security?

ANSWER

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

(a): As per information furnished by Unique Identification Authority of India, no such breach has been reported from the Aadhaar database maintained by it.

The Indian Computer Emergency Response Team (CERT-In) has apprised that a few instances of websites publishing Aadhaar related information of residents, gathered by them from outside the Aadhaar ecosystem, have come to notice. Action in accordance with law is taken in such instances as and when reported.

(b) and (c): Does not arise.

(d): Government has taken the following measures to enhance the cybersecurity posture and prevent such breaches:

(i) On observing a data breach or data leak incident, CERT-In notifies the affected organisations along with remedial actions to be taken and coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as law enforcement agencies.

(ii) CERT-In issues alerts and advisories on latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.

(iii) Cyber Crisis Management Plan formulated by CERT-In for implementation by all Ministries and Departments of the Central / State Governments and their organisations and critical sectors help to counter cyber-attacks and cyber terrorism.

(iv) CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks.

(v) All government websites and applications are audited with respect to cyber security and compliance with the Government of India Guidelines for Websites prior to their hosting.

(vi) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(viii) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

****