PRS LEGISLATIVE RESEARCH

Standing Committee Report Summary

Digital Payment and Online Security Measures for Data Protection

- The Standing Committee on Communications and Information Technology (Chair: Mr. Prataprao Jadhav) presented its report on 'Digital Payment and Online Security Measures for Data Protection' on February 8, 2024. Key observations and recommendations of the Committee include:

- **Increase in online financial frauds:** The Committee noted that there has been a significant increase in the number of cases and amount of money lost in cybercrime. The number of cybercrime complaints rose from 9.7 lakh in 2022 to 11.5 lakh in 2023. Financial frauds are about 60% of the total complaints. Financial frauds worth Rs 5,574 crore were reported between January and October 2023, significantly higher than 2022 (Rs 2,296 crore in full year). Types of financial frauds include customer care number frauds, KYC-based frauds, and Aadhaar enabled Payment Systems (AePS) based frauds.

- The Committee observed that a multipronged approach is needed, which involves all concerned Ministries, in preventing cyber-crime. It recommended the Ministry of Home Affairs to constitute a nodal agency which houses representatives of all the agencies involved.

- **AePS-based crimes:** An AePS facilitates customers to carry out transactions from their Aadhar-linked accounts using biometric authentication. The Committee noted that frauds using AePS were increasing. The Ministry of Home Affairs submitted that dummy or rubber fingers were being used to falsify biometric authentication using Aadhaar.

- **Recovery of money:** The Committee noted that the amount of money recovered and returned to customers was very low (10.4% between 2021 and 2022). It was also noted that the method for filing complaints was complex and there was a high turnaround time to resolve the complaint. It recommended that the Ministry of Home Affairs streamline the process of returning the amounts frozen to the victims.

- **Region specific crimes:** The Ministry of Home Affairs submitted that a majority of the cyber frauds originated from two locations: Mewat region in Rajasthan, Uttar Pradesh, Haryana, and Jamtara in Bihar and Jharkhand. The Committee noted that a large number of micro-ATMs existed in these areas, leading to siphoning off of money. Thus, the Committee recommended that the Ministry of Electronics and Information Technology (MEITY) to formulate region-specific strategies.

- **Need for stricter punitive measures:** The conviction rate in cases of cyber-crime is very low (0.89% in 2021). The Committee observed that punitive measures have not been very effective in curbing cyber-crimes. It further observed that there is a need for statutory and regulatory overhaul in the domain of cybercrimes with stricter punitive measures.

- **Regulation of fintech platforms:** Fintech applications that dominate the Indian market are owned by foreign entities. The Committee noted that certain fintech apps and platforms were being used for money laundering. Hence, it recommended that there should be a greater focus on the promotion of indigenous fintech apps and platforms. It also noted that the regulation of indigenous platforms would be more feasible, since foreign entities have multiple jurisdictions.

- The Committee also observed that fintech apps/platforms must be utilised to generate awareness about common scams and prevention tactics. The Committee recommended MEITY to come with detailed guidelines for banks/fintech platforms and apps on generating awareness. Such awareness should also be conducted in the local language of a region.

- **Lack of specialised staff:** The Committee noted that a number of vacancies exist in specialised agencies such as CERT-In and CSIRT-Fin. In CERT-In, 26 out of 142 sanctioned posts were empty (27%).

- The Committee recommended that staff of central monitoring agencies and state law enforcement agencies should be trained to cater to the rising demand for cyber security professionals.

- **Cyber attacks on the government:** As per MEITY, various attacks are attempted on government websites every year. In 2022, there were 50 such incidents. Some departments/branches of the government used outdated software. The Committee emphasised on the need to adhere to cybersecurity-related guidelines issued by the Ministry. It also recommended the Ministry to upgrade government infrastructure regarding the handling of cyber threats.

DISCLAIMER: This document is being furnished to you for your information. You may choose to reproduce or redistribute this report for non-commercial purposes in part or in full to any other person with due acknowledgement of PRS Legislative Research ("PRS"). The opinions expressed herein are entirely those of the author(s). PRS makes every effort to use reliable and comprehensive information, but PRS does not represent that the contents of the report are accurate or complete. PRS is an independent, not-for-profit group. This document has been prepared without regard to the objectives or opinions of those who may receive it.

Pratinav Damani
pratinav@prsindia.org

February 29, 2024