Standing Committee Report Summary

Cyber Crime: Ramifications, Protection and Prevention

- The Standing Committee on Home Affairs (Chair: Dr. Radha Mohan Das Agrawal) presented its report on 'Cyber Crime: Ramifications, Protection and Prevention' on August 20, 2025. Cybercrime refers to an unlawful act involving the use of technology and digital systems to commit or facilitate a crime. These include crimes in the cyber space such as theft, fraud, forgery, defamation, hacking, malware distribution, and cyber terrorism. Key observations and recommendations of the Committee include:
- **Comprehensive cybercrime legislation:** The Committee observed that cybercrime laws in India are spread across multiple statutes, creating enforcement and judicial challenges. It recommended creating a cybercrime legislation, which defines cyber offences, addresses issues with emerging technologies, and provides strong penal provisions. It also recommended establishing an Integrated Cybercrime Task Force exclusively for investigating cybercrime.
- **Reviewing the IT Act, 2000:** The Committee noted that many provisions in the Act are bailable and attract low penalties. It also observed that the Act does not have any provision to hold IT intermediaries liable for compensating victims for harm due to inaction. It recommended amending the Act to: (i) impose harsher penalties, (ii) require IT intermediaries to compensate victims, and (iii) empower officers above Inspector rank to investigate cybercrime cases.
- **Consent of states for CBI investigations:** Under the Delhi Special Police Establishment Act, 1946, states must provide general consent for the Central Bureau of Investigation to investigate cases within the state. The Committee noted that the withdrawal of consent by several states has hindered investigations. It recommended that the Ministry consult with state governments which have withdrawn consent, and also suggested amending the Act to empower CBI to investigate cybercrime cases without state consent.
- **AI content:** The Committee noted that deepfakes and the use of AI to create misleading content has increased. It observed that the law does not currently differentiate between user-generated and AI-generated content. It suggested that a framework be established, which mandates all content to be watermarked.
- **Advertisers and telemarketers:** The Committee observed a need to develop a comprehensive verification system for offshore advertisers. It also highlighted an increase in complaints related to unregistered telemarketers. In May 2025, there were around 2.1 lakh such complaints. It recommended developing real-time detection mechanisms to block such unregistered telemarketers. It also suggested maintaining a centralised database on all blacklisted telemarketers to be shared across telecom providers.
- **Protection from financial fraud:** RBI had ordered all banks to migrate to the domain '.bank.in' by October 2025. This is expected to help in identifying the genuineness of banks. The Committee observed that no bank has completed the migration process, and recommended that RBI supervise the process. It also recommended setting a timeline for rolling out a digital payment intelligence platform, for safeguarding the digital payments ecosystem. The Committee observed that despite KYC measures, mule accounts (bank accounts made for committing financial fraud) exist. It recommended exploring the possibility of implementing behavioural biometrics that analyse customer pattern such as typing speed or mouse movement of users to spot unusual activity.
- **Unregistered financial influencers:** The Committee highlighted the growing trend of financial influencers on social media platforms who often promote misinformation in this field. It recommended that social media intermediaries be directed to allow only SEBI-registered financial influencers to provide advice and marketing on social media platforms.
- **Coordination between various organisations:** The Committee noted that there is a need for increased coordination between government agencies, regulators, technology platforms, and civil society for knowledge sharing and capacity building in the cyber space. It also recommended: (i) creating expert verticals within TRAI, and (ii) establishing State Cybercrime Coordination Centres in all states/UTs.
- **International cooperation:** The Committee observed that there is a no statutory mandate to enable timely data disclosure from foreign service providers, where important data is stored outside India. It also noted that relying on voluntary cooperation and treaty processes slow down cybercrime investigations. It recommended establishing enforceable legal and diplomatic measures for timely data disclosure. It also suggested setting up a 24x7 unit for coordination with foreign agencies. Further, it recommended developing secure and interoperable intelligence sharing platforms.

Shirin Pajnoo
shirin@prsindia.org

August 31, 2025