Int. Cybersecur. Law Rev. (2021) 2:57–64
https://doi.org/10.1365/s43439-021-00026-7

Square pegs, round holes, and Indian cybersecurity laws

Aadya Misra · Mathew Chacko

Received: 8 March 2021 / Accepted: 10 March 2021 / Published online: 6 April 2021

Abstract India, with one of the world's largest software manpower infrastructures, is also one of the countries with the highest number of hacks, ransomware attacks, and other cybersecurity incidents. Significant ambiguity arises out of the lack of a comprehensive cybersecurity framework, with many sectoral regulations and penal codes interacting with one another in an often confusing manner. This article attempts to provide an overview of laws, regulations, and policies that contribute to the legal framework that underlies cybersecurity requirements in India, and identify issues that arise out of this scattered approach.

Keywords India · Data protection · Information security · Legal · Financial services

1 Introduction

India, with one of the world's largest software manpower infrastructures, is also one of the countries with the highest number of hacks, ransomware attacks, and other cybersecurity incidents [1]. In 2020, many of these incidents involved the unauthorised access and dissemination of millions of data points, ranging from the data of 22 million users of an online education platform [2] to the payment data of 35 million users of a leading payment gateway [3]. The Indian government has been particularly indifferent to cybersecurity concerns, with Aadhar, its flagship national

A. Misra (✉)
School of Law, CHRIST (Deemed to be) University, Bangalore, India
E-Mail: aadya.misra@spiceroutelegal.com

M. Chacko
National Academy of Legal Studies and Research, Shamirpet, India
E-Mail: mathew@spiceroutelegal.com

digital identity (ID) project, and Aarogya Setu, its Covid-19 response app, being significantly insecure offerings in the market [4].

Despite significant judicial censure[1] over the government's and the legislature's inability to pull together a constitutional mandated data protection, privacy, and cybersecurity law, India's legal regime continues to adopt a scattered approach, with many laws dating back to a time when one would not find an entry for the word "computer" in a dictionary. In many instances, the enforcement authorities and the judiciary struggle to resolve disputes at the cutting edge of technology with laws and principles drawn from 19th century statutes.

Indian cybersecurity law is a palimpsest of laws including but not limited to:

- The Indian Penal Code, 1860,
- The Information Technology Act, 2000,
- Various sectoral regulations.

Each of these interact with each other in a fascinating (and strangely, unchoreographed) manner. However, for the purposes of this article, we focus on the Information Technology Act, 2000 and on various sectoral regulations. The Indian Penal Code, 1860—while called into action—was not designed to address cybersecurity issues, and its application frequently causes more confusion and often leads to inequitable resolutions.

2 The Information Technology Act, 2000

2.1 Reasonable security practices and procedures

Under the Information Technology Act, 2000 (IT Act), companies are required to implement "reasonable security practices and procedures" that are designed to protect information from unauthorised access, damage, use, modification, disclosure, or impairment. The government has implemented this section by issuing the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[2] These rules are commonly referred to as the SPDI Rules and are significant as they also set out the country's existing data protection requirements.

Under the SPDI Rules, an entity is considered to have complied with "reasonable security practices and procedures" if it has implemented policies and practices that contain managerial, technical, operational, and physical security measures to protect information assets.[3] In addition, entities are required to have documented information security practices and policies that evidence this implementation. In the event of a security incident, the organisation should be able to demonstrate the implementation of the measures contained in its policies.

[1] Justice K. S. Puttaswamy (Retd.) v. Union of India (2017). Supreme Court Cases, vol. 10, pp. 328.

[2] Ministry of Communications and Information Technology (2011) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules.

[3] Rule 8. In: SPDI Rules (2011).

The SPDI Rules do not impose specific cybersecurity standards: instead, organisations are required to decide for themselves the scope of measures that they must adopt. However, the rules identify ISO 27001 as a standard that would be considered a reasonable security practice or procedure.[4]

2.2 Offences

Companies that cause wrongful loss due to their negligence in the implementation of reasonable security practices and procedures are liable to pay compensation to aggrieved individuals, who may file complaints before an adjudicating officer, provided that the claim does not exceed INR 50,000,000.[5] In turn, the adjudicating officer is required to conduct an inquiry and award compensation as he or she deems fit. Claims that exceed such amounts are heard by courts that have monetary jurisdiction over such thresholds. Provided that the order is made with the consent of the parties to the dispute, appeals against the orders of an adjudicating officer are heard by the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), a body that was initially set up to adjudicate disputes within the telecom sector. Appeals against decisions of the TDSAT are heard before High Courts of respective states in the country.

In addition to negligence in the implementation of reasonable security practices and procedures, the IT Act identifies additional cybersecurity offences. For example, unauthorised access, extraction, damage, disruption, or denial of services in respect of computers and computer networks are offences under the IT Act, as are intentionally tampering with source codes that are required to be maintained under law, identity thefts, and dishonestly receiving stolen computer resources or communication devices.[6] Each of these offences are separately punishable with both imprisonment and fines.

2.3 CERT-In

The IT Act notably establishes a nodal authority that serves as the national government agency for cybersecurity matters in India.[7] Called the Indian Computer Emergency Response Team and commonly referred to as CERT-In, the agency's primary functions include undertaking analyses of cyber incidents, the provision of alerts and forecasts in this regard, and the issuance of emergency measures to tackle and coordinate response activities for cybersecurity incidents.

CERT-In is also the nodal agency that manages security incidents and offers support services to affected organisations. The scope of its support varies, and depends, among other factors, on the severity of the incident, the affected entity, and its resource capability during the occurrence of the incident.

[4] Rule 8. In: SPDI Rules (2011).

[5] The Information Technology Act (2000) Penalties, compensation and adjudication. In: The Information Technology Act, Sec. 46 (1-A).

[6] The Information Technology Act (2000) Offences. In: The Information Technology Act, Chapter XI.

[7] The Information Technology Act (2000) Offences. In: The Information Technology Act, Sec. 70-B.

Unlike several other jurisdictions that require a harm-based approach to determine whether a security incident should be reported to relevant authorities, the IT Act and rules issued thereunder mandatorily require certain types of security incidents to be reported to CERT-In.[8] A comprehensive list of these incidents includes: targeted scanning or probing of critical networks or systems; a compromise of critical systems or information; unauthorised access of information technology systems or data; defacement of websites; intrusions into websites; unauthorised changes to websites; malicious code attacks; attacks on servers; identity thefts; spoofing; phishing attacks; denial of service and distributed denial of service attacks; attacks on critical infrastructure, supervisory control and data acquisition (SCADA) systems, and wireless networks; as well as attacks on applications like e-governance and e-commerce.[9]

The law does not prescribe a timeline for reporting security incidents, but notes that it should be done within a reasonable time to ensure that there is scope for timely action. There are no expressly prescribed penalties for non-compliance with reporting requirements.

2.4 Protected systems

Critical information infrastructure under the IT Act comprises computer resources that have a significant impact on national security, economy, public health, or safety. In this regard, the government has the right to classify systems that impact critical information infrastructure as protected systems, authorise individuals who may access protected systems, and prescribe information security practices and procedures for such protected systems. In addition, the government has established a nodal agency, called the National Critical Information Infrastructure Protection Centre (NCIIPC), to oversee the protection of critical information infrastructure in India.

Presently, protected systems in India are only those that relate to government functions; electronic systems for private commercial activities have not yet been prescribed as protected systems. All protected systems are required to follow the guidelines published by the NCIIPC from time to time, which include the appointment of a chief information security officer and the implementation of planning, implementational, and operational controls, disaster recovery and business continuity protocol controls, as well as reporting and accountability controls.

2.5 Intermediaries

Intermediaries—which include internet, network, and telecom service providers, web hosting service providers, search engines, payment sites, and online marketplaces among other types of digital players[10]—are bound by additional cybersecurity obligations under the IT Act. First, they are required to undertake certain due dili-

[8] Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules (2013) Reporting of incidents. In: CERT-In Rules, Rule 12 (1) (a).

[9] Rule 12. In: Form to report Incidents to CERT-In, CERT-In Rules (2013).

[10] The Information Technology Act (2000) Definitions. In: The Information Technology Act, Sec. 2 (w).

gence while offering their services. Specifically, they are required to contractually require users not to use their services to affect the functionality of computer resources through the introduction or use of technology tools. Second, the IT Act specifically codifies their obligation to cooperate with the government and its agencies in their efforts to investigate, detect, and prevent cybersecurity offences. Third, intermediaries are required to share details of cybersecurity incidents with CERT-In.

Intermediaries are provided certain "safe harbours" to sidestep liabilities that may arise from users' misuse of their resources. For example, intermediaries are not liable for temporary, transient, or immediate storage of information within their network that does not involve human editorial control and that is an intrinsic feature of the intermediary's service.[11] Separately, immediate compliance with the government's instructions in respect of users' offences would limit an intermediary's liability.

3 Sectoral regulations

Sectoral regulations on cybersecurity are common in India. Regulations have been issued in respect of the following sectors: (a) financial services, (b) health services, (c) telecommunications, (d) insurance, and (e) securities law. These regulations continue to be fairly "light touch." An overview of certain regulations follows.

3.1 Financial services

The Reserve Bank of India (RBI), India's central bank, has imposed cybersecurity requirements on various regulated entities—these requirements include mandatory breach notifications, regular audits, threat assessments, and implementation of anti-phishing technology. Banks, for example, are required to create a comprehensive cyber crisis management plan that sets out preparedness indicators and mandates the sharing of all cybersecurity information incidents with the RBI.[12]

The RBI has been at the forefront of multiple enforcement actions including fines on banks and on alternative financing institutions.

3.2 Health

The Government has prescribed the Electronic Health Records Standards (EHR Standards) under the Clinical Establishment (Regulation and Registration) Act, 2010.[13] The EHR Standards are based on global standards and mandate ISO/HL7, ISO/IEC 27002, and ISO/TS 14441:2013.

[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021) Due diligence to be observed by intermediary. In: Due diligence by an intermediary, Rule 3.

[12] Reserve Bank of India (2016) Cybersecurity Framework in Banks. RBI/2015-16/418 DBS.CO/CSITE/BC.11/33.01.001/2015-16.

[13] Ministry of Health and Family Welfare (2016) Electronic Health Records Standards. Notification Q-11011/3/2015-eGov.

In 2020, the government launched the National Digital Health Mission, a policy initiative to create an ecosystem to improve the efficiency of the healthcare system through the exchange of health information. Under this mission, the government has mandated the adoption of ISO/TS 17975:2015 for consent management and the International Standard on Fast Healthcare Interoperability Resources (FHIR) R4 Specification for the electronic exchange of healthcare information.[14]

3.3 Securities market

Stock exchanges, depository participants, asset management, and mutual funds companies are required to implement comprehensive policies that address cybersecurity and cyber resilience, and their approach to cybersecurity should be modelled on the NCIIPC's principles.[15] These organisations are also required to set up information technology committees, designate senior officials to oversee compliance with cybersecurity requirements, and implement technical measures to protect assets and infrastructure.

3.4 Insurance

In 2017, the Insurance Regulatory and Development Authority of India (IRDAI), the country's insurance regulator, issued significant guidance on cybersecurity requirements for insurers that include implementation of adequate processes to identify and mitigate risks, setting up information security committees and teams with the assistance of lawyers, and notifying security incidents to both CERT-In and IRDAI.

Notably, insurers are also required to implement necessary safeguards to ensure that unregulated service providers are adequately bound by these requirements.[16]

3.5 Telecom sector

The Telecom Regulatory Authority of India closely regulates organisations that offer telephone networks or internet services and prescribes security and infrastructure requirements as a condition for operation.

Detailed information security requirements apply to licensed telecom service providers. These entities can only use network elements that comply with prescribed standards that include ISO/IEC 15408, ISO 27000, 3GPP, and 3GPP2 security standards, among others.[17] Certifications in this regard can only be undertaken by authorised agencies in India, unless specifically approved by the Department of

[14] Ministry of Health and Family Welfare (2019) Standards and Regulation. In: National digital health blueprint, p. 33.

[15] Securities and Exchange Board of India (2018) Cyber Security & Cyber Resilience framework for Stock Brokers/Depository Participants. Cir. SEBI/HO/MIRSD/CIR/PB/2018/147.

[16] Insurance Regulatory and Development Authority of India (2017) Guidelines on Information and Cyber Security for Insurers. IRDA/IT/GDL/MISC/082/04/2017.

[17] Ministry of Communications and IT Department of Telecommunications (2012) Scope of license. In: Unified License Agreement, Cl. 2.

Telecommunication. Further, organisations must undertake regular audits and have in place organisational policies and practices on security management. As a condition for operation, service providers are required to contractually ensure that their vendors and suppliers comply with information security requirements.

4 Enforcement trends

In recent years, the TDSAT has played an active role in awarding damages to aggrieved individuals. Most cases in this regard have arisen in respect of negligence by financial institutions to implement reasonable security standards and safeguards. In general, damages awarded have not exceeded actual loss together with interest.

Within the financial services sector, the RBI has imposed penalties on financial institutions for non-compliance with its cybersecurity requirements, with penalty amounts of up to INR 10,000,000.[18] As a general observation, the RBI does play an active role in imposing penalties for cybersecurity requirements; enforcement actions are more commonly witnessed under the IT Act and the SPDI Rules. Notably, any imposition of penalty by the RBI on a banking company precludes the initiation of legal proceedings against the company before courts of law.

There have been recent government policy decisions: in 2020, it launched the National Cyber Crime Reporting Portal that would enable citizens to report cybercrimes online, which would then be accessed by the appropriate law enforcement agencies.

5 The need for a national cybersecurity regulation

As a general observation, this piecemeal approach to cybersecurity has resulted in much confusion, with cybercrimes often being prosecuted under widely worded 19th century statutes, with corporations being unable to derive normative guidance from the often confused tapestry of regulations and offenders getting away in the space between the cracks. A more comprehensive and instructive cybersecurity law, aided by specialist regulation on an as-needed basis, is the need of the hour. Otherwise, courts, enforcement agencies, and regulators will continue to attempt to mould old regulations in ways in which they were not intended to be moulded, and struggle to address many of the challenging cybersecurity issues of the day.

References

1. Thomas KS (2020) Rise in ransomware hacking makes India the second most attacked country globally. https://www.theweek.in/news/biz-tech/2020/10/06/rise-in-ransomware-hacking-makes-india-the-second-most-attacked-country-globally.html. Accessed 15 Feb 2021

[18] Reserve Bank of India (2018) Reserve Bank of India imposes monetary penalty on Indian Bank. Press Release 2018–2019/1345.

2. Ahmad S (2020) Unacademy data hacked, names and passwords put on sale: security firm. Business standard. https://www.business-standard.com/article/companies/unacademy-s-database-hacked-information-of-11-million-users-compromised-120050701280_1.html. Accessed 15 Feb 2021
3. Singhal N (2021) Amazon, Swiggy payments partner Juspay suffers data breach—3.5 crore records compromised. Business Today. https://www.businesstoday.in/technology/news/amazon-swiggy-payments-partner-juspay-suffers-data-breach—35-crore-records-compromised/story/426987.html. Accessed 15 Feb 2021
4. Banerjee P (2020) French hacker finds security issue in Aarogya Setu, says Rahul Gandhi was right. Mint. https://www.livemint.com/technology/tech-news/french-hacker-finds-security-issue-in-aarogya-setu-says-rahul-gandhi-was-right-11588697775275.html. Accessed 15 Feb 2021