



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBERSECURITY LAWS IN INDIA: ARE THEY ADEQUATE?



INTRODUCTION

The digital revolution in India has affected various aspects of life and interactions. Programs such as Digital India, use of UPI, online banking, ecommerce and digital governance make technology a regular element of daily activities. More and more enterprises are migrating to the cloud computing environment. At the same time, the government has been able to make some of its services and transactions available on the Internet. Nevertheless, the digital revolution has not only changed people's lives, but also increased the scale of cyber threats. Phishing, ransomware, identity theft, financial fraud, data breaches and even attacks on critical infrastructure became a common phenomenon. In light of all of the above, one might ask a

question: are India's cyber security laws enough to ensure the safety of individuals, businesses and even national security?

India has elaborated its legislative system of dealing with cybercrimes, based mainly on the IT Act, 2000 and Digital Personal Data Protection Act, 2023. There is an extensive body of law and regulating institutions, which constitutes the base of cyber security governance in India. However, the dynamics of development of technologies raises doubts regarding the readiness of the above framework to cope with modern challenges.

Cyber Security Legislation in India

As opposed to other nations that have passed specific cyber security laws, India lacks a dedicated Cyber security Act. In India, the cyber security legislation comprises a number of Acts, regulations and frameworks.

The IT Act 2000 as amended in 2008 forms the key feature of Indian cyber law. Though initially formulated for facilitating electronic commerce and recognition of electronic records and digital signatures, it has since been extended to cover cybercrimes. The IT Act criminalizes cybercrimes such as unauthorized access of computer system, hacking, identity theft, and online cheating and cyber terrorism. Key provisions in the IT Act are Section 43 & 66 covering unauthorized access/hacking; Sections 66C & 66D relating to identity theft/cheating by personation using computer system; and Section 66F on cyber terrorism carrying life imprisonment among other harsh penalties.

One major addition to India's digital laws is the Digital Personal Data Protection (DPDP) Act, 2023, which provides a legal framework for the processing of digital personal data. The Act mandates organizations to process personal data in a lawful manner, take reasonable security measures, and inform the Data Protection Board and concerned individuals about specific personal data breaches. The law imposes heavy financial penalties on violators, with the highest penalty being ₹250 crore for some violations relating to security measures.

The Indian Computer Emergency Response Team (CERT-In) is the national agency responsible for responding to cyber incidents in India. CERT-In provides security advisories, coordinates the responses to cyber incidents, and increases cyber security readiness. Under the 2022 Directions, certain organizations are mandated to report specified cyber incidents within six hours of coming to their knowledge and maintaining certain logs for cyber security purposes. These laws and institutions make up the framework for cyber security in India.

Why Existing Laws May Not Be Enough?

Despite the fact that there have been considerable developments in India's legal framework, there are still some gaps that need to be addressed.

The first problem is connected with the fact that IT Act, 2000 was developed when technology was completely different. Even considering the amendments introduced in 2008, the law is already old and does not cover many aspects of modern life and technology, especially artificial intelligence, generative AI, applications for block chain technology, cloud computing on a large scale and Internet of Things (IoT). As a result, new forms of cybercrime like deep fake enabled fraud, AI assisted phishing, ransomware attacks, cryptocurrency extortion, and cybercrimes targeting smart devices often have to be dealt with through provisions related to hacking, cheating, and identity theft.

Another issue is enforcement of existing laws. It requires advanced technical skills, digital forensics and coordinated efforts of multiple organizations to conduct an investigation into cybercrimes. In addition, many cybercrimes are transnational in nature and thus are complicated to investigate and prosecute due to issues of jurisdiction. While cybercrime units have been formed in many Indian states, there are still some problems with enforcement.

It is not only about having laws but implementing them. Gathering, storing, and presenting digital evidence has proved to be difficult since the electronic evidence could have been tampered with, encrypted, or distributed in different jurisdictions through cloud servers. Another problem is that India's cyber security legislation is primarily a reactive one and not preventive. Majority of the provisions in Indian cyber security law punish those who engage in cybercrime or whose personal information is at risk after the crime has taken place. Even though the DPDP Act provides greater security for the personal information of the Indians, there is no all-encompassing cyber security legislation that would set certain minimum cyber security standards in all industries including SMEs, which are the targets of many cyber-attacks but often do not have sufficient cyber security infrastructure.

Lastly, public awareness is still a problem. A majority of cybercrimes take place because the victims provide sensitive information voluntarily after receiving it via phishing emails, phone calls, or other social engineering methods. No amount of legislation could change the situation without educating the public on digital literacy and cyber security awareness.

The Way Forward

With the growing digital economy of India, it is imperative to modernize the country's cyber security framework.

Firstly, it would be prudent for India to pass a Cyber security Act that would be specific to technologies like artificial intelligence, deep fakes, ransomware, cryptocurrency offenses, and supply chain attacks among others. This can ensure that there is a clearer set of cyber security obligations for private and public organizations.

In addition, enforcing the laws already on the books should be enhanced through better cyber forensic laboratories, special cybercrime investigation units, judicial training and capability development, as well as cooperation with foreign governments and technology companies among other initiatives.

However, cyber security should not be left entirely up to the government. It is necessary for businesses to strengthen their cyber security measures, audit and train employees. On the other hand, individuals have to practice good cyber security habits through password creation, multi-factor authentication, software updates and avoiding phishing scams.

Conclusion

There is no denying that India has done quite well in making legal provisions to combat cyber security issues through the use of IT Act, 2000, the Digital Personal Data Protection Act, 2023, and CERT-In as an institution. All of these make for a good legal basis of regulation of cybercrimes and response to cyber incidents.

However, the fast changing nature of cybercrimes poses a problem with the existing legal regime. The IT Act, even though relevant, is from a time when these AI-enabled attacks, ransomwares, and complex digital ecosystems did not exist. Recent amendments, like the DPDP Act, have ensured better protection of data, but India requires more in terms of cyber security legal regime.