14 India's Cybersecurity and Data Privacy Ecosystem: Improving Governance in the Digital Age

Dr. Minal Sharma*
Head of Department & Assistant Professor, ICFAI School of Liberal Arts, The ICFAI University Jaipur.
*Corresponding Author: smeenal18@yahoo.com

Abstract

Education is the imparting of knowledge, skills, and attitudes and it takes many forms. Formal education may be imparted in a structured institutional setting, such as schools and colleges, using the planned curriculum. Non-formal education on the other hand is organized but does not take place in schools and informal education refers to casual learning through experience. Formal and non-formal education is divided into several levels, such as ECCE, primary education, secondary education and tertiary education. There are many determinants for whether education works. There are other classifications concerning methodology of teaching (such as, teacher-centred versus student centred approaches to the curriculum), and subject matter (such as, language education, science education, and physical education).

Keywords: Cybersecurity, Indian Government, Digital Ecosystem, Legal Framework.

Introduction

India is getting better at keeping its computer systems and personal information safe. This is because India is using computers and the internet a lot now. The government made a law called the Information Technology Act in 2000. This law was the step in making rules for using computers and the internet in India. It helped people know what to do when they buy or sell things online and what happens if someone does something on the computer. But as computers and the internet became a part of daily life, in India the government realized it needed to make more rules to keep everything safe and fair. Indias computer systems and personal information are still a concern so the country is working to make its cybersecurity and data privacy better.

The government formed the Non-Personal Data Committee in 2019. That was a big change. This showed that the government understood Non-Personal Data had its set of problems to deal with not just Personal Data. One big step forward was when the Digital Personal Data Protection Act was passed in 2023. The Digital Personal Data Protection Act is really important because it wants to make sure Non-Personal Data and Personal Data are safe and that the people in charge are responsible for what they do, with the Non-Personal Data and Personal Data.

Together, these initiatives—covering personal and non-personal data governance, surveillance oversight, public sector data access, and cyber incident response—demonstrate India's commitment to building a secure and rights-based digital ecosystem. This article analyses India's cybersecurity and data privacy trajectory by examining legislative reforms, institutional developments, judicial interventions, and emerging challenges within a global regulatory context.

Methodology

This paper applies a qualitative research approach based on extensive reading of primary and secondary sources. The legislative texts are enunciated into laws and proclamations of the government, committee reports, government policy documents and judicial interpretations on cyber security and related data protection aspects in India. Secondary sources include scholarly writings and conversations.

The book analyses changes in jurisdiction of laws, regulatory bodies and court judgments to provide a full picture of the Indian cyber security system. The paper also has an example of a case in the financial and banking sector cyber security incidents. It draws from the government private sector and independent cyber security experts to identify gaps and make policy recommendations.

Key Developments in Cybersecurity and Data Governance

- **Non-Personal Data Committee**

In September 2019 the Ministry of Electronics and Information Technology made a committee called the Non-Personal Data Committee. This committee was supposed to figure out how to handle issues with -personal data. The Non-Personal Data Committee came out with a report in 2020. This report said that we need rules to manage data that's not about specific people and is combined with other data. The committee said that rules, for -personal data should be part of the bigger laws that protect data. This means the Ministry of Electronics and Information Technology wants to make sure all data is regulated in a way including non-personal data.

- **Data Privacy Standards**

In December 2020 the Bureau of Indian Standards came out with a standard called IS 17428. This IS 17428 standard is about data privacy. It helps organisations figure out how to keep peoples information safe. The IS 17428 standard lists out what

organisations must do and what they should do to protect peoples data. This helps make sure that Indias rules for data are in line with what other countries doing. The IS 17428 standard is really important for data privacy, in India.

- **Review of Surveillance Laws**

People are worried about the government spying on them through means. This is why a judicial committee was formed in October 2021. The digital surveillance issue is a deal. The committee is looking into the laws that're already in place to see if they are good enough. They want to make sure that peoples privacy is protected. The committee has to think about how to balance the need for state security, with the need to protect privacy. The judiciary has a role to play in this. They have to make sure that the government does not spy on people without a reason. The digital surveillance laws need to be looked at.

- **Public Sector Data Policy**

The Ministry of Electronics and Information Technology, which is also known as MeitY made the India Data Accessibility and Use Policy available to the public in February 2022. This policy is meant to help people access the data that the government has collected in a way.

The main goal of the India Data Accessibility and Use Policy is to make things more transparent and to get people to think of ideas. It also wants to make sure that government departments share data, with each other in a manner.

- **CERT-In Directions**

In April 2022 CERT-In made some rules that say companies have to tell them about certain cybersecurity incidents, within six hours. This means companies have to report cybersecurity incidents keep data for a while and work together to respond to incidents. This will help India be better prepared for cybersecurity problems and improve Indias national cybersecurity preparedness by making sure cybersecurity incidents are reported on time.

- **Privacy as a Fundamental Right**

Privacy is a deal, in India when it comes to the internet and computers. The thing is, a lot of information is being collected and shared across the country and even outside of it. For a time India did not have a good law to protect peoples personal information. This meant that people were worried that their information could be used in the way and that there was no one to really stop it from happening. Indias data protection is still an issue because of this.

The Supreme Court helped fix a problem when it said that privacy is a really important part of the right to life under Article 21 of the Constitution. Even though the court did this we still have problems making sure privacy and national security work together especially when it comes to watching people. We really need to make sure

there are rules and someone is keeping an eye on things to make sure everything is fair. The Supreme Court said that privacy is part of the right, to life and now we need to make sure that privacy is protected when the government is trying to keep us safe.

- **The Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act of 2023 is a law that sets rules, for how digital personal data's used in India. This law is important because it helps balance what individuals want with what companies need to use data for. The Digital Personal Data Protection Act of 2023 clearly says what Data Fiduciaries can and cannot do which is a part of this law. The Digital Personal Data Protection Act of 2023 is trying to make sure that individual rights are respected while also letting companies use data in a way.

The law gives Data Principals the right to see their data fix any mistakes and have their data completely removed. It also helps them when they have a complaint. If the rules are broken the people responsible have to pay a fine. The law also makes big Data Fiduciaries do more to protect data like checking their data and seeing how it affects people. The law is especially careful with childrens data. It requires permission, from parents or guardians to collect or use this data.

The Data Protection Board is in charge of making sure the rules are followed. They have the power to look into problems give fines to people who break the rules and help figure out disagreements, about the Data Protection rules.

Challenges and Criticisms

The Act is considered to be very modern. It has still been criticized. The rules that companies must follow may be too hard for businesses and startups which means they have to spend more money to operate. The parts of the Act that deal with moving data across borders may make it tough for companies to do business with countries. Also some parts of the Act are not clear which means that people may interpret them in ways and this can cause delays when it comes to enforcing the Act. The Act is still a problem because of these issues, with the Act.

Addressing these issues requires tiered compliance mechanisms, clearer transfer guidelines aligned with global standards, and detailed regulatory guidance.

Case Study: Cybersecurity in Banking

India's Banking Sector shows us how fast emerging technologies can introduce new threats to businesses that were once considered secure. As more consumers use online banking and mobile applications to manage their finances, banks are now storing and managing millions of accounts and thousands of sensitive records (Social Security Numbers, etc.) for consumers throughout India.

In December of 2015, there was a major cyberattack on several Indian Banks that compromised numerous accounts and allowed attackers access to private consumer information.

As a result of these cyberattacks, the Reserve Bank of India has implemented several new rules and regulations to help banks develop and maintain Strong Cybersecurity Measures. These new regulations include requiring banks to perform regular Cybersecurity Audits and to have in place MFA (Multi-Factor Authentication) standards for any unauthorized changes to their computer systems. The Reserve Bank of India has also required that all Banks create an Incident Response Policy to respond to any cyberattack on their organization. This cyberattack illustrates the need for Banks to remain adaptable to an ever-growing and changing climate of regulations and For Banks to continually invest in high-quality Cybersecurity Infrastructure.

Quantum Cryptography and the Future of Cybersecurity

As the complexity of Cyberthreats continues to increase, there is a growing interest in the use of Quantum Cryptography as a possible method of Cybersecurity. Quantum Cryptography utilizes the principles of Quantum Mechanics to create a completely secure communication channel that will be nearly impossible to penetrate with today's Cyberattacks.

However, there are still many obstacles to overcome in terms of cost, infrastructure, and scalability before the widespread deployment and implementation of this technology will be possible. Continued investment into research, and fostering Public and Private Partnerships, in conjunction with working together with Other Nations will play a Major Role in Developing and Implementing Quantum-Safe Technologies in India.

Conclusion

India is at a unique point in Development, in terms of Cybersecurity and Data Privacy. The Digital Personal Data Protection Bill of 2023 marks a significant step toward improving Cybersecurity and Data Privacy. However, there needs to be clear Regulatory Guidelines available to Banks to ensure compliance and that there are strong Enforcement Mechanisms in place to hold Banks Accountable to the New Law.

To build up the digital environment of India, India requires comprehensive legislationstringent adherence to rights protected by the Constitution use of new and emerging technology and collaboration between those who have an interest in the digital ecosystem. If India can plug existing gaps and align with other countries' standards then India will have the capability to establish a robust, secure and innovative digital future.

References

1. Alik, A. (2022). *Data protection compliance and regulatory burdens on small enterprises*. Journal of Information Law and Policy, 14(2), 45–62.
2. Aiengar, S. (2010). *Cyber security in the Indian banking sector*. Banking Law Journal, 82(4), 311–328.
3. Bagga, R. K. (2018). Cyber security challenges in India: An overview. *International Journal of Computer Sciences and Engineering, 6*(5), 221–227.
4. Bamrara, D., Singh, V., & Sharma, R. (2013). Cyber threats in Indian banking: Issues and challenges. *International Journal of Scientific and Research Publications, 3*(2), 1–6.
5. Bureau of Indian Standards. (2020). *IS 17428: Data privacy assurance framework*. BIS.
6. Burman, A. (2020). Data protection and privacy in India: Emerging legal challenges. *Indian Journal of Law and Technology, 16*(1), 1–24.
7. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. (2018). *A free and fair digital economy: Protecting privacy, empowering Indians*. Government of India.
8. Devi, P. (2019). Public–private partnerships in cybersecurity governance. *Journal of National Security Law, 7*(1), 89–104.
9. Dunn Cavelty, M. (2012). Cyber-security and threat politics: US efforts to secure the information age. *Routledge*.
10. Ghate, R., & Agrawal, S. (2017). Emerging cyber threats and India's preparedness. *Defence Studies Review, 12*(3), 56–72.
11. Government of India. (2000). *Information Technology Act, 2000*. Ministry of Law and Justice.
12. Government of India. (2011). *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. Ministry of Electronics and Information Technology.
13. Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice.
14. Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
15. Ministry of Electronics and Information Technology. (2020). *Report of the Committee on Non-Personal Data Governance Framework*. Government of India.
16. Ministry of Electronics and Information Technology. (2022). *India Data Accessibility and Use Policy*. Government of India.
17. Reserve Bank of India. (2016). *Cyber security framework in banks*. RBI.
18. Shairgojri, A. A., & Dar, A. A. (2022). Data protection laws in India: A critical analysis. *Journal of Cyber Law and Policy, 5*(1), 23–41.