International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 30-10-2024, Accepted: 30-11-2024, Published: 15-12-2024
Volume 6, Issue 4, 2024, Page No. 103-107

Legal framework for cybersecurity in India: Overlaps, issues, and challenges

Ashish Sharma[1], Savyasanchi Pandey[2]
[1] Research Scholar, Department of Law, Kalinga University, Naya Raipur, Chhattisgarh, India
[2] Assistant Professor, Department of Law, Kalinga University, Naya Raipur, Chhattisgarh, India

Abstract
India's cybersecurity landscape is governed by a multifaceted legal framework aimed at safeguarding critical information infrastructure, securing data, and mitigating cyber threats. With increasing digitalization across sectors, the demand for comprehensive cybersecurity regulations has intensified. Over the past decade, authorities have introduced various legislative measures to address emerging cyber risks. This paper examines the evolution of India's cybersecurity legal framework, emphasizing the primary legislation that addresses cybercrimes, data privacy, and information security. It also provides a comparative analysis of regulatory frameworks in the USA, EU, and India, identifying significant gaps and weaknesses. The study finds that the current legal framework remains suboptimal, with challenges related to coverage, enforcement, and public awareness. Additionally, overlapping laws and regulations often result in ambiguity and compliance difficulties for stakeholders, underscoring the need for clarity and harmonization in cybersecurity regulations.

Keywords: Cybersecurity, data privacy, information security, it acts 2000, national security policy, legal framework

Introduction

India's rapid digital transformation, characterized by increasing internet penetration and widespread reliance on technology, has led to a surge in cyber threats, particularly in critical sectors like banking, healthcare, education, and governance (Jain, 2023). The nature and volume of cybercrimes have become more sophisticated, with frequent data breaches and cyber-attacks posing significant risks to individuals, businesses, and the broader digital ecosystem. A robust legal framework is crucial to counter these threats and safeguard sensitive data and critical infrastructure. However, developing comprehensive cybersecurity laws is inherently challenging due to the dynamic nature of emerging technologies like artificial intelligence, blockchain, and quantum computing (Singh, 2024) [19]. Legislation that is effective today may become outdated in a short span, creating a persistent gap between existing laws and the evolving cyber threat landscape. Additionally, limited awareness and technical expertise among policymakers, law enforcement agencies, and the judiciary further impede the formulation and enforcement of effective cybersecurity laws. The lack of coordination among various stakeholders, including central and state governments, private sector entities, and international bodies, complicates the regulatory landscape. Inconsistent implementation, overlapping regulations, and a lack of alignment with global standards also undermine the effectiveness of cybersecurity laws. Public awareness regarding digital privacy and data protection remains low. According to a PWC survey, only 16% of Indians are aware of their privacy rights, and over 60% of companies in India engage in questionable data practices. IBM reports a substantial increase in data breach costs for Indian businesses since 2020 (Dar & Wani, 2023) [8]. Protecting personal data is particularly challenging in the context of smart devices and IoT systems, where vulnerabilities can expose sensitive information (Marikyan *et al*., 2024 [13]; Sadonian, 2024; Shahid *et al*., 2022) [18]. Unregulated access to data stored across multiple global network nodes can violate core principles of information security and privacy (P. Romansky & S. Noninska, 2020) [15]. In healthcare, some researchers advocate for linking mental health data with Aadhaar to prevent data breaches (Bondre, Pathare, & Naslund, 2021) [3]. Others suggest adopting frameworks like the OECD policy guidelines, which share similarities with the GDPR, to establish standardized principles and implementation practices (Campbell, 2021) [5].

To address these challenges effectively, regulations must incorporate user rights, oversight mechanisms, and opt-out provisions to prevent discrimination arising from automated decision-making processes. Innovative strategies for securing digital assets and strengthening data privacy frameworks have also been proposed (Chandra, 2024) [6].

The European General Data Protection Regulation (GDPR) can provide valuable insights for refining India's Digital Personal Data Protection Act (DPDPA), 2023 in several key areas, including:

1. **Direct Obligations on Data Processors:** Introducing specific responsibilities for data processors to enhance accountability and ensure data security.
2. **Contractual Protections for Data Processors:** Mandating clear contractual obligations for data processors to align with data protection standards.
3. **Consent Management Requirements:** Implementing stringent guidelines for consent managers to ensure transparency and informed consent.
4. **Right to Compensation for Non-Compliance:** Establishing mechanisms for affected individuals to claim compensation in cases of data breaches or non-compliance.
5. **Defining Significant Breaches:** Clearly defining what constitutes a "significant" breach to promote consistency and transparency in data breach reporting.
6. **Criteria for Significant Data Fiduciaries:** Outlining specific criteria for classifying significant data

fiduciaries and clarifying their responsibilities and obligations.

7. **Appointment of Independent Auditors and Impact Assessments:** Developing a structured methodology for appointing independent auditors and conducting data protection impact assessments to enhance accountability.

8. **Cross-Border Data Transfers:** Revising the framework for cross-border data transfers to align with global data protection standards and facilitate data exchange (Bentotahewa, Hewage, & Williams, 2022; Singh, 2024) [2, 19].

Russia's recent amendments to its data protection laws post-COVID-19 further highlight the urgency for India to strengthen its regulatory framework. A comprehensive data protection policy is essential to ensure that countries, including EU member states, can transfer data to India without legal complications (Mishra & Kapadia, 2020) [14].

Moreover, researchers advocate for leveraging Artificial Intelligence (AI) to address data protection challenges across multiple jurisdictions, potentially enhancing compliance and reducing operational complexities (Kathuria *et al*., 2024) [11]. However, India's digital economy faces increasing compliance challenges due to overlapping cybersecurity regulations issued by different regulatory bodies. Companies are struggling with inconsistent requirements related to breach reporting, audits, and vulnerability assessments, which complicates compliance efforts (Lochab & Agarwal, 2024) [12].

A comparative analysis of data protection frameworks in India and Germany illustrates the contrast in regulatory approaches. Germany's stringent GDPR framework emphasizes user rights and corporate accountability, whereas India's DPDP Act, 2023, seeks to balance data protection with economic and innovation-oriented policies (Arora, 2020) [1]. Despite differing regulatory frameworks, both countries face similar challenges in enforcing data protection laws, managing cross-border data transfers, and adapting to evolving digital threats. The growing complexity of data governance underscores the need for global cooperation and harmonization in data protection frameworks. Adopting global best practices while addressing local challenges can help India develop a robust, adaptive, and forward-looking data protection framework.

Major Cyber Security Laws in India

India's cybersecurity legal framework is a comprehensive structure aimed at protecting information, ensuring privacy, and securing critical infrastructure. It is governed by multiple laws, regulations, and sector-specific guidelines that define cybercrimes, promote security standards, and mandate incident reporting (PwC, 2022). The key legislations are discussed below:

1. Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) is the cornerstone of India's cybersecurity framework. Enacted to prevent cybercrimes and provide legal recognition to electronic transactions, it establishes safeguards for digital signatures and e-commerce. Key provisions include:

- **Section 43:** Imposes penalties for identity theft, data theft, hacking, and unauthorized access to computer systems.
- **Section 66:** Defines cybercrimes such as hacking, identity theft, and cyberstalking.
- **Section 72:** Penalizes unauthorized disclosure of confidential information by a person in a position of trust.
- **Section 72A:** Provides punishment for disclosing personal data without consent, imposing imprisonment of up to three years, a fine up to ₹500,000, or both.
- **Section 69:** Grants the government powers to intercept, monitor, and decrypt data during national security threats.

The 2008 Amendment to the IT Act introduced additional provisions to address cybercrimes and data protection. The amendment focuses on:

- Establishing legal frameworks for digital signatures.
- Strengthening cybersecurity measures and forensic capabilities.
- Safeguarding electronic transactions and monitoring electronic records.
- Requiring intermediaries to report cybersecurity incidents to CERT-In (Computer Emergency Response Team - India).
- Defining security standards for organizations to prevent cyber terrorism, DDoS attacks, and data breaches.

2. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Enacted under the IT Act, the **Privacy Rules, 2011** outline guidelines for safeguarding personal data and sensitive personal information (SPDI). SPDI includes financial information, biometric data, health records, and passwords. The rules mandate:

- Obtaining explicit consent before data collection.
- Informing users about data usage and processing.
- Implementing reasonable security practices to prevent unauthorized access.
- Developing a privacy policy and establishing grievance redressal mechanisms.

While these rules laid a foundation for data protection, they have now been substantially expanded by the Digital Personal Data Protection Act, 2023 (DPDP Act).

3. Digital Personal Data Protection Act, 2023 (DPDP Act)

Enacted on August 11, 2023, the DPDP Act is India's comprehensive data protection law, inspired by global frameworks like the EU's GDPR. It establishes guidelines for the processing of personal data, focusing on:

- **Lawful Data Collection:** Organizations must obtain explicit consent before processing personal data.
- **Data Minimization:** Collect only the data necessary for specific purposes.
- **Data Security:** Implement appropriate security measures to protect data from unauthorized access.
- **User Rights:** Provides individuals with rights to access, rectify, and delete their data.
- **Data Fiduciaries:** Defines significant data fiduciaries and outlines specific obligations and accountability measures.

- **Cross-Border Data Transfers:** Specifies conditions for transferring personal data outside India, aligning with global standards.
- **Independent Audits:** Mandates independent audits to assess data protection measures.

The DPDP Act addresses emerging concerns over data misuse, cyber threats, and digital surveillance, balancing individual privacy rights with the operational needs of businesses and government entities (Christopher, 2021; Sadonian, 2024) [7].

4. National Cyber Security Policy (NCSP) 2013

The **NCSP 2013** was introduced to establish a secure cyberspace and protect critical infrastructure in sectors like banking, defense, and telecommunications. It focuses on:

- Promoting cybersecurity awareness and public-private partnerships.
- Building indigenous cybersecurity capabilities.
- Establishing frameworks for implementing risk management and incident response mechanisms.
- Proposing the creation of the National Critical Information Infrastructure Protection Centre (NCIIPC) to safeguard critical assets.

Despite its comprehensive framework, the NCSP 2013 has struggled to keep pace with evolving cyber threats and emerging technologies.

5. National Cyber Security Reference Framework (NCRF) 2023

In response to the increasing sophistication of cyber threats, the government launched the NCRF 2023 in June 2023. The framework provides strategic guidance for critical sectors, including banking, healthcare, and energy, to address cybersecurity concerns. It emphasizes:

- Enhancing incident response mechanisms.
- Promoting cybersecurity standards and audits.
- Encouraging capacity building and training in cybersecurity.

Challenges and Recommendations

India's cybersecurity legal framework has evolved significantly, but it still faces several challenges:

- **Rapid Technological Advancements:** Emerging technologies like AI, quantum computing, and blockchain pose new risks that existing laws struggle to address.
- **Overlapping Regulations:** Multiple regulations lead to inconsistencies and compliance challenges for businesses (Lochab & Agarwal, 2024) [12].
- **Cross-Border Data Transfers:** India's current framework lacks clear guidelines for international data transfers, hindering global data exchange (Mishra & Kapadia, 2020) [14].
- **Lack of Awareness and Expertise:** Policymakers and enforcement agencies often lack the technical expertise required to effectively enforce cybersecurity laws.

To bridge these gaps, India can draw on global best practices, particularly the GDPR, to strengthen its legal framework. Key areas for improvement include:

- Establishing direct obligations for data processors.
- Implementing standardized consent management practices.
- Defining significant breaches to ensure consistent incident reporting.
- Enhancing data fiduciary accountability through regular audits and data protection impact assessments.

Addressing these challenges requires continuous updates to existing laws, greater stakeholder engagement, and international cooperation to align with evolving global data protection standards.

Comparative Analysis of Cyber and Data Protection Laws in India, USA and EU

The cyber security legal framework in India is still evolving compared to countries like the USA and EU. The cyber security regulatory framework in countries like India, the UK, the USA and the EU reflect the distinctive cultural, legal and technological landscape in these regions (Ekadshi, 2023) [10]. The main law for the protection of data in India is the Digital Personal Data Protection (DPDP) Act, 2023, which primarily focuses on safeguarding personal data and regulating its processing and maintenance. This legislation is inspired by the General Data Protection Regu- lation (GDPR) 2016 which is one of the most comprehensive regulations on a global basis. The compliance and penalties imposed by DPDP are less stringent compared to the ones in the EU and USA e.g. the penalties for non-compliance are 4% of global turnover for business enterprises in the EU. The regulatory approach to data protection in the USA is sector-specific. To quote, the laws dealing with data protection are the Health Insurance Portability and Accountability Act (HIPAA) for healthcare and the Gramm-Leach-Bliley Act (GLBA) for financial services. California Consumer Privacy Act, 2018 (CCPA), grants consumers significant control over the personal data collected by the businesses from them. Information Technology Act, 2000, the first law in India suffers from the problems of technical expertise and availability of resources. In the EU the Directive on Attacks against Information Systems and NIS2 coupled together deal with the cybercrime regulatory framework across mem- ber states. Computer Fraud and Abuse Act,1986 (CFAA) deals with offences involving unau- thorized access to computer systems. The USA also has strong public-private partnerships to combat cyber threats. National Critical Information Infrastructure Protection Centre (NCIIPC) has been established to safeguard critical infrastructure in India. However, the legal framework for protecting critical sectors like energy, finance, and transportation is still developing, and their implementation remains unsatisfactory. In the EU, the NIS2 directive has provided for stringent security measures for critical infrastructure operators and requires member states to establish Computer Security Incident Response Teams (CSIRTs). The EU also emphasizes cross- border collaboration to address threats to critical infrastructure. The USA has a well-established framework for critical infrastructure protection, led by the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). Laws like the Cyber- security Information Sharing Act (CISA) encourage information sharing between the government and private sector to enhance resilience.

The CERT in India is majorly responsible for the enforcement and compliance of cyber security regulatory procedures and is still evolving in terms of expertise and resources. The EU ENISA (European Union Agency for Cybersecurity) has a strong, sophisticated mechanism for cyber security compliance. The USA primarily rests on technological expertise and active involvement of the private sector enterprises for cyber security and data protection. Despite the stylised sophisticated cyber security legal framework and data security, the EU suffers from the problems of overlapping mandates, e.g. GDPR and NIS2 mandates for critical infrastructure for cyber security and incident reporting suffer from the problems of duplicity, increasing the administrative costs and making it unaffordable to small enterprises. Also, much is needed to enhance the public perception of GDPR (Marikyan *et al*., 2024) [13]. In the member states of the EU, the EU- wide regulations and the cybersecurity legal framework in the member states vary, making the compliance task complicated. For business enterprises dealing in multiple jurisdictions, a lot of patchwork is required, which increases the risks of non-compliance and enhances the possibility of disputes. It has been observed that organisations suffer from the problem of reconciling the differing security standards across regulatory frameworks. In the USA, the regulations are sector- specific and sometimes there is confusion between the federal and state regulations. The best standards practice is yet to evolve in the USA. However, India can draw inferences from the best practices and make changes in regulations wherever required.

Problems and Challenges

The Information Technology Act, 2000 (IT Act) is the primary legislation governing cybersecurity in India. Initially enacted to regulate e-commerce and electronic transactions, the IT Act now serves as the foundational framework for addressing cybercrimes. However, with the rise of sophisticated cyber threats such as ransomware attacks, AI-driven threats, and breaches involving advanced technologies like blockchain and quantum computing**,** the IT Act is increasingly viewed as inadequate.

Despite multiple amendments, the Act falls short in addressing emerging cyber threats effectively. The penalties for cyber offenses under the IT Act are often criticized as being too lenient to serve as a deterrent, leading to an uptick in cyber fraud, data breaches, and financial crimes.

Experts emphasize the urgent need for a dedicated cybersecurity law that comprehensively addresses key areas such as:

1. **Incident Response:** Establishing a standardized framework for reporting and managing cybersecurity incidents.
2. **Digital Forensics:** Defining clear guidelines for evidence collection, preservation, and analysis in cybercrime investigations.
3. **International Cooperation:** Facilitating data sharing and cross-border collaboration to combat transnational cybercrimes.
4. **Cyber Governance:** Assigning specific responsibilities to regulatory agencies for effective enforcement and coordination.
5. **Data Protection and Privacy:** Integrating robust data protection measures to prevent data breaches and unauthorized data access.

Currently, the enforcement of cyber laws is fragmented across multiple agencies, resulting in inconsistent implementation and regulatory overlap**.** A comprehensive cybersecurity law would streamline enforcement, reduce ambiguities, and align India's legal framework with international standards. This would not only strengthen India's cyber resilience but also foster greater trust in its digital infrastructure.

Conclusion

India's cybersecurity legal framework has undergone significant transformation over the past decade. The National Cyber Security Policy (NCSP) has made substantial efforts to address emerging cyber threats. However, the rapidly evolving nature of cyber threats, inadequate infrastructure, and inconsistent implementation continue to pose significant challenges to regulatory efforts.

Currently, India's cybersecurity regulations are fragmented**,** with various agencies managing different aspects of cyber governance. This lack of coordination creates enforcement challenges and complicates compliance for stakeholders. Drawing on international frameworks such as the GDPR**,** India can develop more comprehensive and streamlined regulations tailored to its unique socio-economic landscape. Public awareness of data privacy in India is still relatively low compared to global standards, underscoring the need for targeted initiatives to educate citizens about their data protection rights. While India's Digital Personal Data Protection Act (DPDP), 2023 aligns with global data privacy standards, certain provisions require customization to address local challenges effectively. Despite efforts to create a robust cybersecurity legal framework, overlapping laws and inconsistent enforcement continue to undermine regulatory effectiveness. Establishing a harmonized legal framework with clear guidelines, coordinated enforcement mechanisms, and capacity-building initiatives can significantly improve India's cybersecurity posture and enhance public trust in digital systems.

References

1. Arora K. Privacy and data protection in india and germany: A comparative analysis, 2020.
2. Bentotahewa V, Hewage C, Williams J. The normative power of the gdpr: A case study of data protection laws of south asian countries. SN Comput Sci,2022:31:83. https://doi.org/10.1007/ s42979-022-01079-
3. Bondre A, Pathare S, Naslund J. Protecting mental health data privacy in india: The case of data linkage with aadhaar. Glob Health Sci Pract,2021:9:467–480. https://doi.org/10.9745/GHSP- D-20-00346
4. Burman A. Understanding india's new data protection law, 2023. [Accessed 27 February 2025].
5. Campbell C. A review of data protection regulations and the right to privacy: The case of the us and india. Manohar Parrikar Institute for Defence Studies and Analyses, 2021.
6. Chandra A. Strengthening india's cybersecurity and data privacy landscape: A comprehensive overview. Indian Journal of Public Administration,2024:70:466–478. https://doi.org/10.1177/ 00195561241271616
7. Christopher K. The path to recognition of data protection in india: The role of the gdpr and international standards. National School of India Review,2021:33:69–91.
8. Dar M, Wani S. Covid-19, personal data protection and privacy in india. Asian Bioeth Rev,2023:15:125–140. https://doi.org/10.1007/s41649-022-00227-0

9. Deloitte. Cybersecurity and cyber resilience framework (cscrf) for sebi-regulated entities, 2024.
10. Ekadshi DM. Comparative analysis of cyber security laws of india, united states, and United Kingdom. International Journal of Law,2023:9:88–91.
11. Kathuria Y, Ruhani V, Tyagi M, Jain V. Protecting data privacy in the age of ai: A com- parative analysis of legal approaches across different jurisdictions. AIP Conference Proceedings, 2024, 040007. https://doi.org/10.1063/5.0234669
12. Lochab H, Agarwal S. Companies grapple with costs, complexity of overlapping cybersecurity laws. The Economic Times, 2024.
13. Marikyan D, Papagiannidis S, Rana OF, Ranjan R. General data protection regulation: A study on attitude and emotional empowerment. Behaviour Information Technology,2024:43:3561–3577. https://doi.org/10.1080/0144929X.2023.2285341
14. Mishra N, Kapadia Y. Lack of jurisprudence in data protection laws in india vis a vis the russian scenario, 2020. https://blog.ipleaders.in/lack-jurisprudence-data-protection-laws-india/.
15. P. Romansky R, S Noninska I. Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering,2020:17:5288–5303. https://doi.org/10.3934/ mbe.2020286 pwc. (2022). A comparison of cybersecurity regulations: India [Accessed 27 February 2025].
16. Robb L, Candy T, Deane F. Regulatory overlap: A systematic quantitative literature review.
17. RegulGov,2023:17:1131–1151. https://doi.org/10.1111/rego.12504 Sadonian, L. (2024). Gdpr's influence on indian data protection practices.
18. Shahid J, Ahmad R, Kiani A, Ahmad T, Saeed S, Almuhaideb A. Data protection and privacy of the internet of healthcare things (iohts). Applied Sciences,2022:12:1927. https ://doi.org/10.3390/app12041927
19. Singh N. Data protection and privacy challenges in digital age in india. White Black Legal International Law Journal, 2024, 16.