

# **Benchmarking Technical Provisions in Global Data Protection Frameworks: A Systematic Meta-Review**

**Chisomo Amurhola Tolani<sup>1\*</sup>, J Pareek<sup>2</sup>, L K Sharma<sup>3</sup>**

<sup>1</sup>Computer Science, Gujarat University, Ahmedabad, India,

<sup>2</sup>Computer Science, Gujarat University, Ahmedabad, India,

<sup>3</sup>ICMR- National Institute of Occupational Health, Ahmedabad, India.

## **ABSTRACT**

The increasing reliance on interconnected devices, particularly through the Internet of Things (IoT), necessitates the development of technically enforceable data protection frameworks. This study presents a systematic meta-review of five major global data protection frameworks: The General Data Protection Regulation, the National Institute of Standards and Technology, the Brazilian general data protection law, China's Personal Information Protection Law, and India's DPDP Act and India IT Act with SPDI Rules. The results show that GDPR and PIPL offer comprehensive technical mandates, while NIST provides a robust technical blueprint for operational privacy management. Brazil's LGPD lacks detailed mandates for certain technical protections, while India's IT Act and SPDI Rules require improvement due to lack of technical specificity and IoT alignment. The study contributes to the global data protection discourse by offering a comparative benchmarking tool and highlighting critical gaps in technical enforceability, especially for developing economies. It recommends an integrated, technically operable framework to ensure privacy, resilience, and interoperability in a hyper-connected digital age.

**Keywords:** Data protection Frameworks, GDPR, IoT Security, Internet of Things, Technical Compliance.

## 1. INTRODUCTION

As digital transformation accelerates across industries, it becomes important to safeguard personal data and taking it as a critical priority. It can be noted that, “the protection of personal data has become a cornerstone of trust, security, and regulatory governance,” which reflects the growing expectations of both consumers and regulators[1][2]. There is a great increase in exposure of personal and sensitive data to breaches, unauthorized access, and unethical processing due to the rapid proliferation of connected devices through the Internet of Things (IoT)[3][4].

Jurisdictions worldwide have implemented robust data protection frameworks to guide organizations in the secure and lawful collection, storage, processing, and transfer of personal data as a response to the threats[2][5][6].

The European Union’s General Data Protection Regulation (GDPR), the United States’ National Institute of Standards and Technology (NIST) Privacy Framework, Brazilian general data protection law (LGPD), China’s Personal Information Protection Law (PIPL), and India’s Digital Personal Data Protection (DPDP) Act of 2023 are among the most influential frameworks of data protection. Whereas the GDPR has set a global benchmark for rights-based, purpose-limited data governance, other countries / regions have adapted their frameworks based on national priorities and regulatory philosophies that guide data protection.

In contrast to many developed economies, there is lack of a centralized national IoT policy in India, which is particularly noteworthy. IoT-related privacy and security requirements in India are scattered across several policies such as the National Digital Communications Policy, Smart Cities Mission, and sectoral guidelines issued by agencies like the Telecom Regulatory Authority of India (TRAI). This fragmentation presents practical challenges for ensuring technical uniformity in data protection across connected systems and networks. The recently enacted DPDP Act aims to fill some of these gaps, but the absence of a holistic IoT governance regime continues to constrain technical enforcement[7].





From these contextual disparities, we have adopted a systematic meta-review approach to comparatively analyze five frameworks across 21 technical dimensions, which include encryption, access control, pseudonymization, breach notification, and privacy-by-design. This review paper

benchmarks each of the frameworks based on individual technical provisions and then assesses readiness to secure personal data in IoT ecosystems.

This paper contributes to the global data protection discourse by introducing a technical comparative lens for evaluating legal and non-legal frameworks. The gap between policy design and technical enforceability can be bridged by this review thereby offering a benchmarking tool, that policymakers can use to assess and improve data governance models. For developing countries this is particularly relevant as the regulatory and technical readiness lags behind digital growth. By highlighting gaps, such as the absence of pseudonymization, breach response, and interoperability, the study presents priority areas for strengthening data protection in IoT-driven environments.

## 2. METHODOLOGY

A systematic meta-review approach was adopted and guided by the PRISMA 2020 framework, to evaluate the technical robustness of five global data protection frameworks: GDPR (EU), DPDP (India), NIST (USA), LGPD (Brazil), and PIPL (China). A structured search of legal documents, government portals, academic databases, and policy reports has been conducted using keywords that are related to data protection, technical compliance, and IoT governance.

After screening 60 records and applying inclusion/exclusion criteria, five core frameworks were selected for detailed analysis and other records were used also used throughout the study. Each framework was assessed against 21 predefined technical dimensions, which includes encryption, breach notification, privacy by design, event logging, and cross-border data transfer. A three-level coding scale was used to classify each technical aspect such as for a fully implemented (double ticks,  ), partially implemented (single tick, ), or not clearly addressed (a cross, ). The results are synthesized into a comparative matrix (Table 1) and supported by a PRISMA flow diagram which offer insights into the alignment and divergence of technical mandates across jurisdictions.

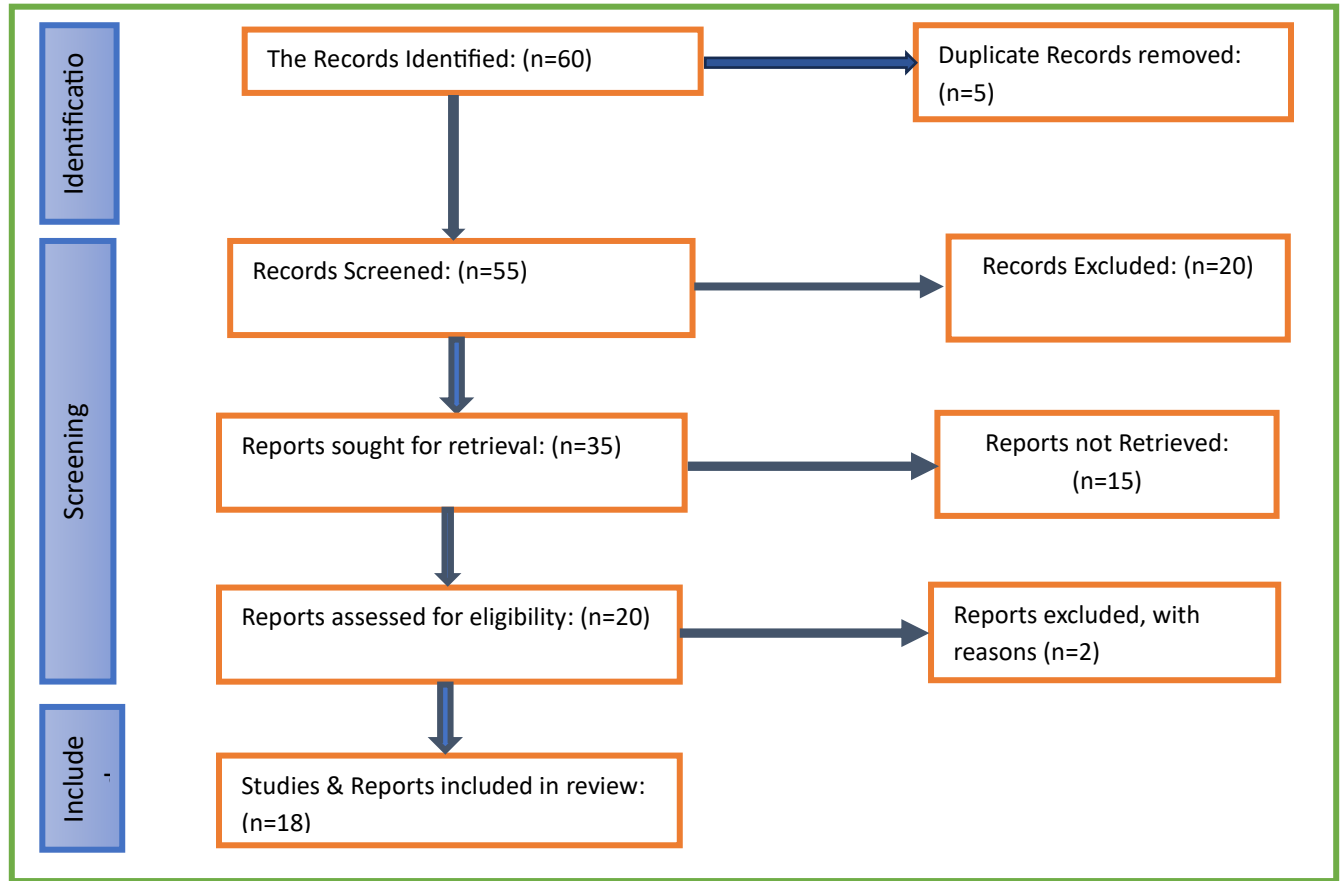


Figure 1: PRISMA Flow Diagram

### 3. RESULTS AND ANALYSIS

To provide a structured understanding of how global data protection frameworks tackle key technical aspects, we conducted a side-by-side comparative matrix of GDPR, DPDP (India), NIST, LGPD (Brazil), and PIPL (China) across 21 technical aspects. These aspects, encryption, access control, breach notification, event logging, and interoperability, are crucial for ensuring data protection, particularly in intricate IoT ecosystems. Each framework's alignment with these dimensions was assessed using a three-tier scale: The table categorizes the frameworks as Fully Implemented (✓✓), Partially Implemented (✓), and Not Clearly Addressed (✗). The analysis indicates both the strengths and weaknesses of each framework in converting legal mandates into actionable technical requirements.

No.	Technical Aspect	GDPR	DPDP (India)	NIST	LGPD	PIPL
1	Data Minimization	☑☑	☑	☑	☑☑	☑☑
2	Encryption (At Rest/In Transit)	☑☑	☑	☑☑	☑	☑☑
3	Access Control	☑☑	☑	☑☑	☑	☑☑
4	Pseudonymization	☑☑	✗	☑	☑	☑
5	Data Breach Notification	☑☑	☑	☑	☑☑	☑☑
6	Consent Mechanisms	☑☑	☑	☑	☑☑	☑☑
7	Purpose Limitation	☑☑	☑	☑	☑☑	☑☑
8	Data Retention Policies	☑☑	☑	☑	☑	☑
9	Cross-Border Data Transfers	☑☑	☑	✗	☑☑	☑☑
10	Data Subject Rights	☑☑	☑	☑	☑☑	☑☑
11	Accountability Mechanisms	☑☑	☑	☑☑	☑	☑☑
12	Security Measures (General)	☑☑	☑	☑☑	☑	☑☑
13	Auditing & Logging	☑☑	✗	☑☑	☑	☑
14	Privacy by Design	☑☑	☑	☑	☑	☑
15	Incident Response Requirements	☑☑	☑	☑☑	☑	☑☑
16	Cybersecurity-by-Design	☑	✗	☑☑	☑	☑
17	Vulnerability Management	☑	✗	☑☑	☑	☑
18	Authentication & Access Control	☑☑	☑	☑☑	☑	☑
19	Cyber Resilience	☑	✗	☑☑	☑	☑
20	Event Logging	☑	✗	☑☑	☑	☑
21	Interoperability & Standards	☑	✗	☑☑	☑	☑

Table 1: Framework Compliance Across 21 Technical Aspects

The Table 1 reveals a clear technical depth gradient, with GDPR, PIPL, and NIST scoring consistently high in binding technical mandates. GDPR and PIPL stand out for their robust enforcement of encryption, breach reporting, and privacy by design. NIST, being a technical

framework rather than a legal regulation, excels in Accountability, cyber resilience, vulnerability management, Interoperability and logging just to mention a few.

Brazil's LGPD, though modeled after GDPR, shows minor lags in standardization and auditing provisions. It lacks the detailed security architecture mandates present in GDPR or NIST but makes up with strong emphasis on consent, purpose limitation, and breach notifications.

In contrast, India's DPDP, while rights-based in theory, exhibits limited specificity on technical safeguards, particularly in the absence of a centralized IoT policy. Critical technical aspects such as pseudonymization, vulnerability management, event logging, and interoperability are either vaguely defined or entirely missing in current DPDP guidance. This gap is particularly consequential for IoT ecosystems where distributed device networks demand consistent enforcement of security baselines.

During the comparative we noted that, although India enacted the Digital Personal Data Protection (DPDP) Act in 2023 to establish a unified framework for personal data governance, it lacks explicit technical mandates tailored to Internet of Things (IoT) ecosystems. In contrast to other frameworks evaluated in this study, the DPDP Act does not yet operationalize provisions such as privacy-by-design, data minimization, or technical interoperability standards—dimensions critical to securing IoT environments.

Therefore, for the purpose of this comparative technical analysis, we thought of replacing Indian DPDP Act, with India's *Information Technology Act, 2000*, along with its subordinate *SPDI Rules (2011)*, for more representative legal instruments as these continue to regulate digital ecosystems in India, particularly through provisions under Section 43A of the IT Act, which mandates "reasonable security practices" for handling sensitive personal data[8]. This substitution ensures a more accurate and technically grounded comparison across jurisdictions.

We now present an updated comparative technical analysis that includes IT Act, 2000 and SPDI Rules (2011).

Technical Aspect	GDPR	NIST	LGPD	PIPL	India (IT Act + SPDI Rules)
Encryption (At Rest/In Transit)	✓✓	✓✓	✓✓	✓✓	✓
Pseudonymization/Anonymization	✓✓	✓	✓	✓✓	✗
Privacy by Design and by Default	✓✓	✓✓	✓	✓✓	✗
Data Minimization	✓✓	✓	✓	✓✓	✗
Breach Notification Mechanism	✓✓	✓	✓✓	✓✓	✓
Access Control Mechanisms	✓✓	✓✓	✓	✓✓	✓
User Consent Mechanism	✓✓	✓	✓✓	✓✓	✓
Purpose Limitation	✓✓	✓✓	✓✓	✓✓	✓
Data Retention Policy	✓✓	✓	✓	✓	✓
Right to Access	✓✓	✓	✓✓	✓✓	✓
Right to Correction/Rectification	✓✓	✓	✓✓	✓✓	✗
Right to Erasure/Deletion	✓✓	✓	✓	✓✓	✗
Data Portability	✓✓	✓	✓	✓	✗
Automated Decision-Making and Profiling	✓✓	✓	✓	✓	✗
Cross-border Data Transfer Restrictions	✓✓	✗	✓✓	✓✓	✗
Third-party Data Sharing Rules	✓✓	✓	✓	✓✓	✓
Logging and Auditability	✓✓	✓✓	✓	✓	✗
Security Certification Requirements	✓	✓✓	✗	✓	✗
Accountability and Governance	✓✓	✓✓	✓	✓✓	✓
Risk Assessment Protocols	✓✓	✓✓	✓	✓	✗
Interoperability Standards	✓	✓✓	✗	✗	✗

Table 2: Technical Compliance Comparison (Including India's IT Act and SPDI Rules)

Both the GDPR (EU) and PIPL (China) continue to demonstrate the highest levels of technical specificity. GDPR is notable for its binding mandates on encryption, pseudonymization, data subject rights, and interoperability. PIPL stands out for its strict localization requirement, graded data classification, and strong enforcement mechanisms.

The NIST Privacy Framework (USA), despite its non-legislative status, excels in operational areas like logging, risk management, and organizational accountability. Its modular structure allows flexible adoption across sectors and maturity levels but lacks universal legal enforceability.

Brazil's LGPD shows moderate strength. While it closely follows GDPR in areas such as breach notification, consent mechanisms, and purpose limitation, it is comparatively weaker in security certification requirements, interoperability standards, and enforcement readiness.

After replacing the Indian DPDP Act 2023, the technical comparative analysis across 21 core privacy and security dimensions' reveals that, India's IT Act, 2000 and SPDI Rules, 2011 demonstrate the lowest technical depth and coverage among the frameworks studied. While they include general requirements for "reasonable security practices" and some basic consent and access control provisions, they lack clarity on critical controls such as pseudonymization, data portability, automated processing oversight, and privacy by design. Still the absence of technical interoperability standards, breach response protocols, and structured risk assessments places India at a disadvantage—particularly as its digital economy and IoT landscape rapidly evolve.

This gap is particularly concerning as India scales initiatives such as 5G deployment. Smart cities. And the Digital Public Infrastructure (DPI) ecosystem. Without enforceable technical standards, these projects remain vulnerable to data breaches and regulatory misalignment with global best practices.

#### 4. DISCUSSION

We have seen how the comparative analysis has highlighted the substantial variation in the technical rigor and enforceability of global data protection frameworks. While GDPR and PIPL exhibit a relatively holistic approach with enforceable mandates across nearly all 21 technical aspects, others particularly India's IT Act and SPDI Rules they do struggle with specificity and completeness in technical articulation, especially in areas central to secure IoT deployment.

##### *4.1 GDPR and PIPL: Technically Prescriptive Frameworks*

The General Data Protection Regulation (GDPR) leads in terms of prescriptive technical requirements. Features such as encryption (Art. 32), pseudonymization (Art. 4 & 25), privacy by design (Art. 25), and data subject rights (Art. 15–22) are not only detailed in their definition but



are legally binding[9][10][11]. GDPR's ability to integrate both legal principles and technical enforcement mechanisms makes it a reference point for global data governance.

Similarly, China's Personal Information Protection Law (PIPL) demonstrates robust technical governance, with concrete mandates around cross-border transfer assessments, localization for critical data, and stringent security measures (Art. 51–55). China's use of graded classification of personal data and sector-specific standards (e.g., cybersecurity law) further complements the PIPL in addressing technical controls[12][13][14][15].

#### *4.2 NIST: A Technical Blueprint, Not a Law*

The NIST Privacy Framework, while not a legal instrument, excels in defining a modular, implementation-ready architecture. Its Core structure—covering Identify, Govern, Control, Communicate, and Protect—offers practical guidance on event logging, vulnerability management, and cyber resilience, aspects often under-defined in legal frameworks. However, NIST lacks binding authority and relies heavily on organizational willingness and maturity to implement its controls[16]. As we have seen in the table 1 and 2, NIST privacy framework does not cover cross-border data transfer restrictions. This is because NIST is a voluntary, non-legislative framework from the United States that provides technical and organization guidance for managing privacy risks. As for example if an organization in the U.S wants to address cross-border transfer compliance, they must pair NIST with legal frameworks such as the EU-U.S. Data Privacy Framework or contractual tools like Standard Contractual Clauses.

#### *4.3 Brazil's LGPD: Inspired but Incomplete*

Brazil's LGPD, heavily modeled on GDPR, reflects substantial progress in consent, breach notification, and data subject rights. However, it does not mandate encryption or vulnerability response protocols with the same precision as its European counterpart. Enforcement mechanisms, while centralized under the ANPD (National Data Protection Authority), are relatively new and still maturing. The lack of detailed implementation guidelines hinders consistent enforcement, and the technical mandates are not as clearly articulated as in GDPR or PIPL.

#### *4.4 India's IT Act and SPDI Rules: Outdated Legal Basis, Technically Shallow*

Given the technical shortcomings of India's DPDP Act (2023)[7] and its current lack of IoT-specific provisions, the study instead evaluated India's Information Technology Act, 2000[8] and its SPDI Rules (2011), as these are legal instruments currently in force and still governing digital environments in India.

While Section 43A of the IT Act introduces the concept of "reasonable security practices," the law falls short on technical specificity. The SPDI Rules offer limited guidance on data retention, consent, and access control, but omit critical controls such as pseudonymization, encryption, event logging, or interoperability standards[17]. There is also no binding requirement for privacy by design, data portability, or automated processing protection, all of which are essential for managing data in IoT ecosystems.

Furthermore, India lacks a national IoT policy, and current governance relies on fragmented sectoral guidelines (e.g., MeitY), most of which are either voluntary or still under draft stages. Though initiatives like the TEC 31318:2021 and IoT System Certification Scheme represent progress, they lack comprehensive enforceability across sectors[18][7]. As India pursues ambitious digital infrastructure goals, such as smart cities, 5G rollout, and Digital Public Infrastructure (DPI)—the absence of enforceable, cross-sectoral technical mandates presents a major vulnerability.

## **5. CONCLUSION**

In this paper we have presented a systematic technical comparison of five prominent data protection frameworks, GDPR, PIPL, NIST, LGPD, and India's IT Act with SPDI Rules - across 21 technical aspects. According to the comparison, the GDPR and PIPL frameworks are particularly well-suited to managing increasingly complex and dispersed data ecosystems, especially in the context of IoT environments, because they offer extensive legal and technical protections.

we have also seen that NIST framework, provides a technically sound and adaptable framework that helps organizations operationalize privacy, even though it is not legally binding. Despite being

progressive, we have observed that LGPD needs to be further improved in order to match the strict implementation standards of its European counterpart.

On the other hand, India's IT Act and SPDI Rules, represent an antiquated method of data governance. But the absence of IoT-sensitive provisions, fragmented enforcement mechanisms, and a lack of technical specificity put India at a regulatory disadvantage, particularly as it scales emerging technologies like 5G, AI, and smart cities and advances significant digital public infrastructure initiatives.

In light of these insights, the following suggestions are made:

- i. *For India:* Based on international best practices in GDPR and NIST, immediate policy updates should seek to either completely revamp the current IT legal framework or greatly improve the new DPDP Act, 2023, by incorporating enforceable, IoT-relevant technical provisions.
- ii. *For all jurisdictions:* Future regulations must be technically feasible, interoperable, and verifiable in addition to enshrining data protection principles, particularly in cases where data flows across devices and borders.
- iii. *For researchers and policymakers:* For evaluating the technical depth of national frameworks or directing the creation of sector-specific policies, the 21-aspect comparative model employed in this study can be used as a reusable benchmarking tool.

As data governance becomes a strategic national priority, the convergence of legal mandates and technical safeguards will determine whether frameworks are fit-for-purpose in a world powered by IoT, AI, and pervasive computing. Countries that fail to integrate both will risk lagging in privacy protection, global trade alignment, and digital sovereignty.

## REFERENCES

- [1] R. Millman, "Data Privacy and Security Regulations in the Digital Transformation Era," [www.isms.online](https://www.isms.online/data-privacy/data-privacy-and-security-regulations-in-the-digital-transformation-era/). [Online]. Available: <https://www.isms.online/data-privacy/data-privacy-and-security-regulations-in-the-digital-transformation-era/>
- [2] J. S. Far and S. Court, "Advent of Privacy Era in India," 2023.

- [3] I. Coston, E. Plotnizky, and M. Nojournian, “Comprehensive Study of IoT Vulnerabilities and Countermeasures,” *Appl. Sci.*, vol. 15, no. 6, 2025, doi: 10.3390/app15063036.
- [4] N. Gravenor and F. F. Adedoyin, “Information Security Threats in the Internet of Things (IoT),” vol. 25, no. 5, pp. 291–304, 2023, doi: 10.4018/978-1-6684-7207-1.ch015.
- [5] D. A. Harandi, “International Legal Frameworks on Cybersecurity and Data Protection Law,” 2025, [Online]. Available: <https://djilp.org/international-legal-frameworks-on-cybersecurity-and-data-protection-law/>
- [6] A. Mishova, “Data Protection Laws Around the World: A Global Perspective.” [Online]. Available: <https://gdprlocal.com/data-protection-laws-around-the-world-a-global-perspective/>
- [7] Government of India, “Digital Personal Data Protection Act 2023,” *Gaz. India*, no. D1, p. 21, 2023, [Online]. Available: <https://www.meity.gov.in/writereaddata/files/DigitalPersonalDataProtectionAct2023.pdf>
- [8] Indian Parliament, “The Information Technology Act,” pp. 1–36, 2000, [Online]. Available: [https://www.indiacode.nic.in/bitstream/123456789/13116/1/it\\_act\\_2000\\_updated.pdf](https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf)
- [9] L. Baudot and K. Robson, “Regulation,” *Routledge Companion to Crit. Account.*, vol. 2014, no. October 1995, pp. 184–204, 2017, doi: 10.4324/9781315775203-11.
- [10] P. R. GDPR, “The General Data Protection Regulation (GDPR) AN EPSU BRIEFING,” *Gen. data Prot. Regul.*, pp. 1–40, 2018, [Online]. Available: [https://www.epsu.org/sites/default/files/article/files/GDPR\\_FINAL\\_EPSU.pdf](https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf)
- [11] GDPR-Regulations, “Regulation - 2016/679 - EN - gdpr - EUR-Lex.” Accessed: Aug. 07, 2025. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
- [12] W. Privacy and C. Practice, “China Finalises Exemptions to Cross-Border Data Transfer Rules and Eases Restrictions,” no. 3249, pp. 1–8, 2024.
- [13] J. Gong, “China Data Protection and Cybersecurity: Annual Review of 2024 and Outlook

- for 2025 (I) - Bird \& Bird,” 2025. [Online]. Available:  
[https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-\(i\)](https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-(i))
- [14] V. Chaturvedi, “Understanding China’s Personal Information Protection Law (China PIPL),” 2024. [Online]. Available: <https://www.bitraser.com/article/understanding-china-personal-information-protection-law-pipl.php>
- [15] R. Creemers and G. Webstar, “Translation: Personal Information Protection Law of the People’s Republic of China – Effective Nov. 1, 2021,” 2021. [Online]. Available: <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>
- [16] NIST, *NIST Privacy Framework*. 2020. [Online]. Available:  
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>
- [17] MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY, “Section 43A of the Information Technology Act,” *Dep. Inf. Technol.*, vol. 3, no. i, 2011, [Online]. Available: <http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf>
- [18] Government of India, “Code of Practice for Securing Consumer Internet of Things (IoT) TELECOMMUNICATION ENGINEERING CENTER DEPARTMENT OF TELECOMMUNICATIONS MINISTRY OF COMMUNICATIONS GOVERNMENT OF INDIA RELEASE 1.0 Code of practice for securing Consumer Internet of Things (IoT.” [Online]. Available: [www.tec.gov.in/M2M-IoT-](http://www.tec.gov.in/M2M-IoT-)