INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 4 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 4 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-4-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"CORPORATE DATA PROTECTION OBLIGATIONS IN INDIA: A CRITICAL STUDY OF COMPLIANCE AND ENFORCEMENT CHALLENGES"

AUTHOR – PALLAVI DIXIT. STUDENT AT AMITY UNIVERSITY LUCKNOW CAMPUS

BEST CITATION – PALLAVI DIXIT, "CORPORATE DATA PROTECTION OBLIGATIONS IN INDIA: A CRITICAL STUDY OF COMPLIANCE AND ENFORCEMENT CHALLENGES", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (4) OF 2026, PG. 299-313, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The increasing reliance on digital technologies and data-driven business models in India has intensified concerns regarding the protection of personal data and the accountability of corporations handling such information. This research paper examines the legal and regulatory framework governing corporate data protection obligations in India, with a particular focus on compliance requirements and enforcement challenges. It analyses the evolution of data protection laws from the Information Technology Act, 2000 to the more comprehensive regime established under the Digital Personal Data Protection Act, 2023, highlighting the shift from a negligence-based approach to a compliance-driven and accountability-oriented framework.

The study explores key concepts such as corporate accountability, due diligence, data governance principles, and the nature of data breaches, while critically evaluating the obligations imposed on corporations as data fiduciaries. It further identifies significant challenges in implementation, including regulatory capacity constraints, compliance burdens on organisations, delays in breach detection and reporting, and gaps in enforcement mechanisms. Through doctrinal analysis, case law references, and comparative insights from international frameworks, the paper assesses the effectiveness of the current legal regime in ensuring corporate accountability.

The research finds that although the DPDP Act represents a substantial improvement in strengthening data protection and corporate responsibility, its effectiveness is contingent upon robust enforcement, institutional capacity, and clarity in regulatory guidelines. The paper concludes by recommending measures to enhance compliance, strengthen enforcement mechanisms, and promote a culture of responsible data governance. It argues that effective corporate accountability requires moving beyond formal compliance towards proactive risk management and sustained commitment to data protection in India's evolving digital ecosystem.

Keywords: Corporate Data Protection, Data Breach, Corporate Accountability, Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, Compliance, Enforcement Challenges

Chapter 1: Introduction

1.1 Background and Evolution of Data Protection in India

The evolution of data protection in India reflects the country's transition from a limited, sectoral approach to a more structured and rights-based framework. Initially, data protection concerns were addressed under the Information Technology Act, 2000, which primarily focused on electronic governance and cyber offences rather than comprehensive privacy protection. The recognition of privacy as a fundamental right by the Supreme Court **in Justice K.S. Puttaswamy v. Union of India** marked a transformative moment, establishing informational privacy as an essential

component of Article 21 of the Constitution. Following this**, the Justice B.N. Srikrishna Committee (2018)**[580] recommended a dedicated data protection framework, ultimately leading to the enactment of the Digital Personal Data Protection Act, 2023. This progression demonstrates a shift from reactive, negligence-based liability to a proactive regime emphasising accountability, compliance, and individual rights.

1.2 Growth of Digital Economy and Data Risks

India has emerged as one of the fastest-growing digital economies, driven by increasing internet penetration, smartphone usage, digital payment systems, and initiatives like Digital India. According to industry estimates, India's digital economy is expected to reach **$1 trillion by 2030**, reflecting the scale of data-driven activities. However, this growth has been accompanied by a significant rise in cyber threats and data breaches. Corporations now process vast volumes of personal and sensitive data, making them prime targets for cyberattacks such as phishing, ransomware, and identity theft.

Table 1: Growth of Digital Risks in India

Aspect	Trend
Internet Users	Over 800 million users
Digital Payments	Rapid growth via UPI systems
Data Breaches	Increasing frequency and scale
Cyber Threats	Rise in ransomware and phishing attacks

The expansion of digital infrastructure has thus created a dual challenge: enabling innovation while ensuring robust protection of personal data.

1.3 Statement of the Research Problem

Despite legislative developments, significant gaps remain in ensuring effective corporate accountability for data breaches in India. The IT Act framework[581] relied on negligence-based liability, which often proved inadequate due to difficulties in proving fault and limited deterrence. While the DPDP Act introduces a structured compliance and penalty-based regime, concerns persist regarding enforcement capacity, regulatory clarity, and accessibility of remedies for affected individuals. The research problem centres on whether the current legal framework effectively addresses corporate responsibility in data protection or whether practical and institutional challenges continue to undermine its effectiveness.

1.4 Objectives of the Study

The study aims to critically analyse corporate data protection obligations in India and evaluate the effectiveness of compliance and enforcement mechanisms. It seeks to examine the evolution of legal frameworks, assess corporate responsibilities under existing laws, and identify gaps in implementation. Additionally, the research intends to explore challenges faced by corporations in achieving compliance and propose recommendations to strengthen accountability and enforcement.

1.5 Research Questions and Hypothesis

The research is guided by key questions concerning the adequacy and effectiveness of India's data protection regime. It examines whether corporations are sufficiently accountable for data breaches, how the DPDP Act differs from the earlier IT Act framework, and whether the shift to a penalty-based system enhances compliance and deterrence. It also explores enforcement challenges and the role of regulatory authorities. The study is based on the hypothesis that the DPDP Act, 2023 strengthens corporate accountability through a compliance-driven and penalty-based framework; however, its effectiveness is dependent on enforcement mechanisms,

[580] Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

[581] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 3.

institutional capacity, and corporate adherence to data governance principles.

1.6 Scope and Limitations

The scope of this study is limited to corporate data protection obligations within the Indian legal framework, focusing primarily on the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. While the study includes references to international standards for comparative understanding, it does not undertake an exhaustive comparative analysis. Limitations include the recent enactment of the DPDP Act, resulting in limited judicial interpretation and practical enforcement data. Additionally, technical aspects of cybersecurity are discussed only to the extent necessary for legal analysis.

1.7 Research Methodology

The research adopts a doctrinal and analytical methodology, focusing on the interpretation of statutory provisions, judicial decisions, and regulatory guidelines. Primary sources include legislation and case laws, while secondary sources consist of books, journal articles, and government reports. The study also incorporates limited empirical insights from reported data breach incidents and policy documents. This methodology enables a comprehensive evaluation of both theoretical and practical aspects of corporate accountability in data protection.

1.8 Structure of the Paper

The paper is organised into six chapters to ensure a systematic analysis of the subject. Chapter I introduces the research topic and outlines its objectives, methodology, and scope. Chapter II discusses the conceptual framework of corporate data protection and accountability. Chapter III examines the legal framework under the IT Act and the emergence of the DPDP Act. Chapter IV analyses corporate obligations and compliance requirements. Chapter V explores enforcement challenges and practical issues. Finally, Chapter VI presents findings, recommendations, and concluding observations, providing a comprehensive evaluation of corporate data protection obligations in India.

Chapter 2: Conceptual Framework of Corporate Data Protection

2.1 Meaning and Scope of Data Protection

Data protection refers to the legal and regulatory framework governing the collection, processing, storage, and dissemination of personal data to ensure privacy, security, and lawful use. In the Indian context, the scope of data protection has evolved from a limited focus on "sensitive personal data" under the Information Technology Act, 2000 to a broader and more comprehensive regime under the Digital Personal Data Protection Act, 2023[582], which covers all forms of digital personal data. The scope of data protection extends beyond mere confidentiality to include principles such as lawful processing, purpose limitation, data minimisation, and accountability. It also encompasses the rights of individuals, including the right to access, correct, and erase personal data. The increasing reliance on digital platforms has expanded the scope of data protection to include cross-border data flows, cloud storage, and emerging technologies such as artificial intelligence. Thus, data protection today represents a dynamic and evolving field that balances the interests of individuals, corporations, and the state.

2.2 Corporate Accountability in Data Protection

Corporate accountability in data protection refers to the obligation of organisations to ensure compliance with legal standards and to take responsibility for safeguarding personal data throughout its lifecycle. Corporations act as primary custodians of data and are therefore expected to implement robust governance mechanisms, maintain transparency, and ensure that data processing activities are conducted in a lawful and ethical manner. Under modern frameworks such as the DPDP

[582] Digital Personal Data Protection Act, 2023

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Act, accountability is not limited to post-breach liability but extends to proactive compliance, requiring corporations to demonstrate adherence to data protection principles through documentation, audits, and internal controls. The concept is closely linked to the fiduciary role of corporations, where they are expected to act in the best interests of individuals whose data they process. Failure to meet these obligations may result in regulatory penalties, reputational damage, and loss of consumer trust, thereby reinforcing the importance of accountability in the digital age.

2.3 Nature and Types of Data Breaches

Data breaches are incidents involving unauthorised access, disclosure, alteration, or destruction of personal data, which can have serious consequences for individuals and organisations. The nature of data breaches has evolved with technological advancements, becoming more complex and difficult to detect. Breaches can be categorised into three primary types: confidentiality breaches, where data is exposed to unauthorised parties; integrity breaches, where data is altered or corrupted; and availability breaches, where access to data is disrupted. Additionally, breaches may arise from external threats such as hacking, malware, and phishing attacks, as well as internal factors such as employee negligence or malicious intent.

Table 2: Types of Data Breaches

Type of Breach	Description	Example
Confidentiality Breach	Unauthorised disclosure of data	Data leak or hacking
Integrity Breach	Alteration or tampering of data	Database manipulation
Availability Breach	Loss of access to data	Ransomware attack

The increasing frequency and sophistication of such breaches highlight the need for stronger corporate accountability and effective legal frameworks to address these risks.

2.4 Due Diligence and Reasonable Security Practices

Due diligence in data protection refers to the obligation of corporations to take all reasonable measures to prevent data breaches and ensure the security of personal data. This includes implementing technical safeguards such as encryption, firewalls, and intrusion detection systems, as well as organisational measures like employee training, access controls, and incident response planning. Under the IT Act framework, the concept of "reasonable security practices" forms the basis of corporate liability, particularly under Section 43A[583]. However, the determination of what constitutes "reasonable" security is context-dependent and may vary based on the nature of data and the scale of operations. The DPDP Act further strengthens this obligation by requiring corporations to adopt a proactive approach to risk management and compliance. Due diligence is therefore a continuous process that involves regular monitoring, updating of security measures, and adherence to evolving technological standards, making it a key component of corporate accountability.

2.5 Principles of Data Governance

Data governance refers to the framework of policies and practices that guide the management of data within an organisation. It is based on key principles that ensure responsible handling of personal data throughout its lifecycle. These principles include data minimisation, which requires collecting only necessary data; purpose limitation, which restricts data use to specified objectives; accuracy, which ensures data correctness; storage limitation, which mandates retaining data only for as long as necessary; and accountability, which requires organisations to demonstrate compliance with these principles. Effective data governance involves the

[583] Rahul Matthan, Privacy and Data Protection in India, Indian J. L. & Tech.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

establishment of internal structures such as data protection officers, audit mechanisms, and compliance reporting systems[584]. These principles are central to modern data protection laws and play a crucial role in ensuring transparency, reducing risks, and building trust between corporations and individuals. By integrating data governance principles into their operations, organisations can enhance their accountability and ensure compliance with legal requirements.

2.6 Theoretical Foundations of Corporate Liability

The concept of corporate liability in data protection law is grounded in various legal theories that explain how corporations can be held responsible for data breaches and related harms. Strict liability imposes responsibility irrespective of fault in certain statutory contexts, emphasising the need for compliance with legal standards. Negligence-based liability arises from the failure to exercise reasonable care in protecting data, which has traditionally been the basis of liability under the IT Act. Vicarious liability holds corporations responsible for the acts of their employees or agents, reflecting the principle that organisations must ensure proper supervision and control. These traditional theories are complemented by modern regulatory approaches that emphasise accountability, compliance, and deterrence. The shift towards a fiduciary model under the DPDP Act reflects an evolving understanding of corporate liability, where organisations are expected[585] to act in the best interests of individuals and demonstrate proactive compliance. This theoretical foundation provides the basis for understanding the legal framework governing corporate accountability in data protection.

Chapter 3: Legal Framework Governing Data Protection in India

3.1 Overview of the Information Technology Act, 2000

The Information Technology Act, 2000 is the primary legislation governing cyber law in India and provides the foundational legal framework for electronic transactions, digital signatures, and cyber offences. Although its primary objective was to facilitate e-commerce and electronic governance, it also includes provisions that indirectly address data protection and cybersecurity. The Act criminalises unauthorised access to computer systems, data theft, and damage to digital infrastructure, thereby offering a basic level of protection against data breaches. However, the Act does not provide a comprehensive framework for personal data protection, as it lacks clear definitions, rights-based provisions, and structured compliance obligations. Its approach is largely reactive, focusing on penalising wrongful acts rather than preventing them. Despite these limitations, the IT Act[586] laid the groundwork for subsequent developments in India's data protection regime.

3.2 Section 43A and SPDI Rules, 2011

Section 43A of the IT Act introduces the concept of corporate liability for failure to protect sensitive personal data. It provides that a body corporate handling such data is liable to pay compensation if it is negligent in implementing reasonable security practices and procedures, resulting in wrongful loss or gain. To operationalise this provision, the government enacted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These rules define "sensitive personal data," including financial information, passwords, health data, and biometric information, and impose obligations such as obtaining consent, maintaining privacy policies, and ensuring data security.

[584] Paul M. Schwartz, Information Privacy in the Digital Age, 161 Harv. L. Rev. 195 (2000).

[585] Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006).

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

Table 3: Key Features of Section 43A and SPDI Rules

Aspect	Provision
Applicability	Body corporates handling sensitive personal data
Liability	Compensation for negligence
Requirement	Reasonable security practices
Compliance	Privacy policy, consent, data protection measures
Limitation	Applies only to sensitive personal data

While these provisions marked an important step towards corporate accountability, their limited scope and reliance on negligence-based liability reduced their effectiveness in addressing large-scale data breaches.

3.3 Limitations of the IT Act Framework

The IT Act framework has been widely criticised for its inadequacies in addressing modern data protection challenges. One of the primary limitations is its narrow scope, as it focuses only on sensitive personal data and does not cover all categories of personal information. Additionally, the absence of a comprehensive definition of privacy and lack of enforceable rights for individuals weaken its effectiveness. The enforcement mechanism, which relies on adjudicating officers, often suffers from delays, lack of technical expertise, and limited accessibility. The compensation-based model under Section 43A also fails to provide sufficient deterrence, particularly in cases involving large corporations. Furthermore, the Act does not mandate data breach notification, allowing organisations to conceal breaches and avoid accountability. These limitations highlight the need for a more comprehensive and robust legal framework.

3.4 Emergence of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 represents a significant development in India's data protection landscape. It was enacted in response to the growing need for a comprehensive legal framework that addresses the challenges of the digital economy and protects individual privacy. The Act is influenced by global standards and aims to balance the interests of individuals, corporations, and the state. It introduces a rights-based approach, recognising individuals as data principals and corporations as data fiduciaries. The Act also reflects the constitutional recognition of privacy as a fundamental right **in Justice K.S. Puttaswamy v. Union of India.** By establishing clear roles, obligations, and enforcement mechanisms, the DPDP Act seeks to create a structured and accountable data protection regime in India.

3.5 Key Features of the DPDP Act, 2023

The DPDP Act introduces several features that significantly enhance corporate accountability and data protection. It establishes a comprehensive framework governing the processing of digital personal data, including requirements for lawful processing, consent, and data security. The Act mandates that data fiduciaries implement appropriate technical and organisational measures to protect data and prevent breaches. It also introduces a data breach notification mechanism, requiring organisations to inform both regulatory authorities and affected individuals.

Table 4: Key Features of the DPDP Act, 2023

Feature	Description
Data Fiduciary Concept	Defines corporate responsibility
Consent Requirement	Mandatory for data processing
Data Breach Notification	Obligatory reporting of breaches
Penalty Framework	High financial penalties
Regulatory Authority	Data Protection Board of India

These features represent a shift towards a proactive and compliance-driven approach, ensuring that corporations are accountable for their data handling practices.

3.6 Shift from Negligence to Compliance-Based Regime

One of the most significant changes introduced by the DPDP Act is the shift from a negligence-based liability framework to a compliance-based regulatory regime. Under the IT Act, liability depended on proving negligence, which often posed challenges for affected individuals. In contrast, the DPDP Act imposes clear and proactive obligations on corporations, requiring them to implement data protection measures and demonstrate compliance. The introduction of substantial financial penalties for non-compliance enhances deterrence and encourages organisations to prioritise data protection. This shift reflects a broader trend towards accountability-based regulation, where corporations are expected to take responsibility for preventing data breaches rather than merely responding to them. However, the effectiveness of this regime depends on factors such as enforcement capacity, clarity of guidelines, and corporate willingness to adopt robust compliance practices.

Case Law Analysis (Relevant to Data Protection and Corporate Liability)

- Justice K.S. Puttaswamy v. Union of India – Established the **right to privacy as a fundamental right**, forming the constitutional basis for data protection laws in India.
- Shreya Singhal v. Union of India[587] – Though primarily addressing freedom of speech, it highlighted the need for **clear and precise legal provisions** in digital regulation.
- Google India Pvt. Ltd. v. Visaka Industries[588] – Examined **intermediary liability**, emphasising corporate responsibility in online content and data handling.
- Avnish Bajaj v. State (NCT of Delhi) – Addressed **vicarious liability of corporate entities**, laying groundwork for accountability in cyber-related offences.

Chapter 4: Corporate Data Protection Obligations

4.1 Concept of Data Fiduciary and Data Principal

The Digital Personal Data Protection Act, 2023[589] introduces the concepts of "Data Fiduciary" and "Data Principal" as the foundation of corporate data protection obligations. A Data Fiduciary refers to any entity, including corporations, that determines the purpose and means of processing personal data, thereby placing primary responsibility for data protection on such entities. A Data Principal is the individual whose personal data is being processed. This relationship establishes a fiduciary-like duty, requiring corporations to act in the best interests of individuals and ensure fairness, transparency, and accountability in data processing. The classification clarifies roles within the data protection framework and strengthens corporate responsibility by imposing direct obligations on organisations handling personal data.

4.2 Duties and Responsibilities of Corporations

Corporations, as data fiduciaries, are required to comply with a range of statutory obligations aimed at ensuring the lawful and secure processing of personal data. These duties include processing data only for lawful purposes, ensuring data accuracy, implementing appropriate security safeguards, and preventing unauthorised access or misuse. Organisations must also establish grievance redressal mechanisms to address complaints from data principals and ensure transparency

[587] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[588] *Google India Pvt. Ltd. v. Visaka Industries*, (2020) 4 SCC 162.
[589] Digital Personal Data Protection Act, 2023.

in their operations. In addition, certain entities classified as Significant Data Fiduciaries are subject to enhanced obligations such as conducting data protection impact assessments, appointing data protection officers, and undertaking periodic compliance audits. These responsibilities reflect a comprehensive approach to corporate accountability, requiring organisations to integrate data protection into their governance and operational frameworks.

4.3 Consent Mechanism and Data Processing Principles

Consent is a central element of the DPDP Act and serves as the primary legal basis for processing personal data. Corporations are required to obtain free, informed, specific, and unambiguous consent from data principals before collecting or processing their data. The Act also incorporates key data protection principles such as purpose limitation, data minimisation, and storage limitation, which restrict the use and retention of personal data to what is necessary for specified purposes. Individuals are granted rights such as the right to access information, correct inaccuracies, and withdraw consent, thereby enhancing their control over personal data.

Table 5: Key Data Processing Principles

Principle	Description
Consent	Free and informed permission of the individual
Purpose Limitation	Data used only for specified purposes
Data Minimisation	Collection of only necessary data
Accuracy	Ensuring correctness of data
Storage Limitation	Retention only for required duration

These principles ensure that data processing is conducted responsibly and transparently, reinforcing corporate accountability.

4.4 Data Security and Risk Management Practices

Data security is a critical component of corporate obligations under the DPDP Act. Corporations are required to implement appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration, or destruction. These measures include encryption, firewalls, access controls, intrusion detection systems, and regular security audits. Risk management practices such as vulnerability assessments, incident response planning, and employee training are also essential for preventing data breaches. The concept of due diligence requires organisations to continuously monitor and update their security practices in response to evolving threats. Effective risk management not only ensures compliance with legal requirements but also reduces the likelihood of data breaches and associated liabilities

4.5 Data Breach Notification and Incident Response

The DPDP Act introduces mandatory data breach notification requirements, which significantly enhance transparency and accountability. Corporations are required to report data breaches to the relevant regulatory authority and inform affected individuals in a timely manner. This obligation ensures that individuals can take necessary steps to mitigate potential harm, such as identity theft or financial loss. Effective incident response mechanisms are essential for compliance, requiring organisations to detect breaches promptly, contain the impact, and implement corrective measures. The requirement of breach notification also acts as a deterrent, encouraging corporations to strengthen their data protection practices and avoid reputational and financial consequences.

4.6 Penalty Framework and Regulatory Oversight

The DPDP Act establishes a penalty-based enforcement regime, imposing significant financial penalties for non-compliance with its provisions. Unlike the compensation-based approach under the Information Technology Act, 2000, the new framework emphasises deterrence through regulatory sanctions. Penalties may be imposed for failure to implement security safeguards, non-compliance with breach notification requirements, and violation of data protection principles.

Table 6: Comparison of Liability Frameworks

Aspect	IT Act, 2000	DPDP Act, 2023
Nature of Liability	Negligence-based	Compliance-based
Remedy	Compensation	Penalties
Scope	Limited (SPDI)	Broad (all personal data)
Enforcement	Adjudicating Officers	Data Protection Board

Regulatory oversight is carried out by the Data Protection Board of India, which is responsible for monitoring compliance, investigating violations, and imposing penalties. This structured enforcement mechanism enhances accountability and ensures adherence to data protection standards.

Case Law and Practical Insights

- Justice K.S. Puttaswamy v. Union of India[590] – Reinforced the importance of **informational privacy and consent**, forming the basis for corporate obligations.
- Google India Pvt. Ltd. v. Visaka Industries – Highlighted **corporate responsibility in digital environments**, particularly regarding intermediary roles.
- Avnish Bajaj v. State (NCT of Delhi)[591] – Established **vicarious liability of corporations**, relevant for employee-related data breaches.

Chapter 5: Compliance and Enforcement Challenges

5.1 Institutional and Regulatory Constraints

The effectiveness of data protection laws in India is significantly influenced by the capacity of regulatory institutions responsible for enforcement. While the Digital Personal Data Protection Act, 2023 provides for the establishment of the Data Protection Board of India, concerns remain regarding its operational capacity, technical expertise, and independence. Regulatory bodies often face challenges such as limited resources, lack of specialised personnel, and inadequate technological infrastructure, which hinder effective monitoring and enforcement. Additionally, the absence of a well-developed institutional framework for data protection may lead to inconsistencies in decision-making and delays in resolving disputes. These constraints raise questions about the practical implementation of the law and its ability to ensure corporate accountability in data protection.

5.2 Corporate Compliance Burden and Industry Concerns

The introduction of comprehensive data protection obligations has imposed significant compliance burdens on corporations. Organisations are required to invest in advanced cybersecurity infrastructure, implement data governance frameworks, and establish mechanisms for consent management and grievance redressal. While large corporations may have the resources to meet these requirements, small and medium enterprises (SMEs) often struggle due to financial and technical constraints. Additionally, the complexity of regulatory requirements and lack of detailed guidelines create uncertainty in

[590] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

[591] *Avnish Bajaj v. State (NCT of Delhi)*, 150 (2008) DLT 769.

implementation. Industry stakeholders have expressed concerns regarding the cost of compliance, potential impact on innovation, and the risk of heavy penalties for non-compliance. Balancing regulatory objectives with business practicality remains a key challenge in the effective enforcement of data protection laws.

5.3 Issues in Breach Detection and Reporting

Timely detection and reporting of data breaches are critical for mitigating harm and ensuring accountability; however, several challenges exist in this regard. Many organisations lack the technical capability to detect breaches promptly, particularly in cases involving sophisticated cyberattacks or insider threats. Delays in detection can increase the severity of harm and reduce the effectiveness of response measures. Furthermore, corporations may be reluctant to report breaches due to concerns about reputational damage, financial losses, and regulatory penalties. Although the DPDP Act mandates breach notification, practical difficulties such as uncertainty regarding reporting timelines and lack of standardised procedures can hinder compliance. These issues highlight the need for improved technical capacity and clear regulatory guidelines.

5.4 Adjudication Delays and Access to Remedies

The enforcement of data protection laws in India is also affected by delays in adjudication and limited access to remedies for affected individuals. Under the Information Technology Act, 2000, the adjudication process has often been criticised for being slow and inefficient, with limited awareness among individuals regarding their rights and available remedies. While the DPDP Act introduces a more structured enforcement mechanism, concerns remain about potential delays and procedural complexities. Access to justice is further hindered by factors such as lack of legal awareness, high costs of litigation, and limited institutional capacity. Ensuring timely and effective remedies is essential for strengthening corporate accountability and protecting individual rights.

5.5 Gaps in Enforcement and Regulatory Overlaps

Despite the introduction of the DPDP Act, certain gaps in the enforcement framework continue to exist. One major issue is the overlap between different legal provisions and regulatory authorities, which can create confusion and inconsistencies in implementation. For example, provisions under the IT Act and sector-specific regulations may overlap with the DPDP Act, leading to jurisdictional conflicts. Additionally, the absence of detailed rules and guidelines for certain aspects of the Act creates ambiguity and uncertainty for corporations. These gaps can weaken the effectiveness of the legal framework and hinder the achievement of its objectives. Addressing these issues requires harmonisation of laws and clear delineation of regulatory responsibilities.

5.6 Impact on Consumers and Digital Trust

Data breaches have significant implications for consumers, including financial loss, identity theft, and invasion of privacy. Repeated incidents of data breaches can erode public trust in digital platforms and reduce confidence in the digital economy. Corporate failure to protect personal data not only affects individuals but also undermines the credibility of businesses and institutions. The effectiveness of data protection laws is therefore closely linked to their ability to enhance consumer trust and ensure accountability. Strengthening enforcement mechanisms, improving transparency, and ensuring timely redressal of grievances are essential for building trust in the digital ecosystem.

Table 7: Key Compliance and Enforcement Challenges

Challenge	Impact
Regulatory Constraints	Weak enforcement

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Challenge	Impact
Compliance Burden	Increased cost for businesses
Breach Detection Issues	Delayed response
Adjudication Delays	Limited access to justice
Legal Overlaps	Confusion and inconsistency
Consumer Impact	Loss of trust

Case Law and Practical Insights

- Justice K.S. Puttaswamy v. Union of India – Emphasised the need for **strong safeguards and enforcement mechanisms** to protect privacy.
- Shreya Singhal v. Union of India[592] – Highlighted the importance of **clear legal provisions and procedural safeguards** in digital regulation.

Chapter 6: Findings, Recommendations and Conclusion

6.1 Key Findings of the Study

The study reveals that India's data protection framework has undergone a significant transformation from a fragmented and negligence-based regime to a more structured and compliance-oriented system. The earlier framework under the Information Technology Act, 2000 provided limited protection, primarily focusing on sensitive personal data and relying on compensation-based remedies. This approach lacked strong enforcement mechanisms and failed to create sufficient deterrence against large-scale data breaches. The introduction of the Digital Personal Data Protection Act, 2023[593] marks a shift towards a comprehensive regulatory model that emphasises accountability, transparency, and compliance. However, the findings indicate that despite this progress, challenges such as enforcement capacity, regulatory ambiguity, and compliance burdens continue to affect the effectiveness of the framework. The study also highlights that corporate accountability is still evolving and requires stronger institutional support and practical implementation.

6.2 Evaluation of the Legal Framework

The combined framework of the IT Act and the DPDP Act reflects both progress and limitations in India's approach to data protection. While the IT Act laid the foundation for addressing cyber offences and introduced the concept of reasonable security practices, it lacked the scope and depth required to address modern data protection challenges. The DPDP Act addresses many of these shortcomings by introducing clear obligations, a structured enforcement mechanism, and a penalty-based regime. However, certain issues remain, including overlaps between different laws, lack of detailed implementation guidelines, and uncertainty regarding regulatory interpretation. The effectiveness of the framework ultimately depends on its ability to balance the interests of individuals, corporations, and the state while ensuring robust enforcement and accountability.

6.3 Recommendations for Strengthening Compliance

To enhance corporate compliance with data protection laws, several measures can be adopted. First, corporations should invest in advanced cybersecurity infrastructure and adopt best practices such as encryption, regular audits, and risk assessments. Second, organisations must integrate data protection principles into their governance structures by appointing data protection officers and establishing internal compliance mechanisms. Third, there is a need for greater awareness and training among employees to ensure adherence to data protection standards. Additionally, regulatory authorities should provide clear and detailed guidelines to reduce ambiguity and facilitate compliance. Strengthening compliance mechanisms will not

[592] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[593] Digital Personal Data Protection Act, 2023.

only reduce the risk of data breaches but also enhance corporate accountability.

6.4 Policy Suggestions for Effective Enforcement

Effective enforcement of data protection laws requires a coordinated and well-resourced approach. Policymakers should focus on strengthening the institutional capacity of regulatory bodies by providing adequate resources, technical expertise, and independence. The use of technology in regulatory processes, such as automated monitoring and reporting systems, can improve efficiency and transparency. There is also a need to harmonise overlapping legal provisions and ensure consistency in enforcement across different sectors. Developing sector-specific guidelines and encouraging collaboration between regulators, industry stakeholders, and the judiciary can further enhance enforcement effectiveness. These measures will help create a robust and efficient data protection ecosystem.

6.5 Scope for Future Research

The field of data protection is continuously evolving, and several areas require further academic exploration. Future research can focus on the impact of emerging technologies such as artificial intelligence, big data analytics, and blockchain on privacy and corporate accountability. Additionally, studies can examine the effectiveness of enforcement mechanisms under the DPDP Act once sufficient implementation data becomes available. Comparative research on international data protection frameworks can also provide valuable insights for improving India's legal regime. Such research will contribute to the ongoing development of data protection laws and policies.

6.6 Concluding Observations

In conclusion, the evolution of data protection law in India reflects a growing recognition of the importance of safeguarding personal data in the digital age. The transition from the IT Act framework to the DPDP Act represents a significant step towards strengthening corporate accountability and ensuring compliance. However, the success of this framework depends on effective implementation, regulatory capacity, and corporate commitment to data protection principles. By addressing existing challenges and adopting a proactive approach to data governance, India can build a robust data protection regime that enhances trust in the digital economy and protects the rights of individuals.

Chapter 7: Comparative and Future Perspectives in Data Protection

7.1 Comparative Analysis with Global Data Protection Frameworks

A comparative analysis of international data protection frameworks provides valuable insights into the strengths and weaknesses of India's regulatory approach. The General Data Protection Regulation[594] is widely regarded as one of the most comprehensive data protection regimes, emphasising strict compliance, individual rights, and significant penalties for non-compliance. It adopts principles such as privacy by design, accountability, and data protection impact assessments, which have influenced global standards. Similarly, China's Personal Information Protection Law (PIPL) [595]adopts a stringent approach with strong state control and strict obligations on corporations, particularly in relation to data localisation and cross-border data transfers. Japan's Act on the Protection of Personal Information (APPI) reflects a balanced approach, combining regulatory oversight with industry self-regulation. Compared to these frameworks, India's Digital Personal Data Protection Act, 2023 adopts a flexible and evolving model that seeks to balance innovation with privacy protection, though it still requires further development to match global best practices.

[594] General Data Protection Regulation (EU) 2016/679.
[595] Personal Information Protection Law (PIPL), China (2021).

7.2 Cross-Border Data Transfer and Global Compliance Challenges

In an increasingly interconnected digital economy, cross-border data flows have become a critical aspect of corporate operations. Multinational corporations frequently transfer data across jurisdictions for processing, storage, and analysis. However, differences in legal standards and regulatory requirements create significant compliance challenges. The DPDP Act allows cross-border data transfers subject to conditions notified by the government, reflecting a relatively flexible approach compared to stricter regimes like the GDPR. Nevertheless, corporations must navigate complex compliance requirements, including ensuring adequate data protection standards in recipient countries and managing contractual safeguards. The absence of detailed guidelines on cross-border transfers in India may create uncertainty and increase compliance risks for corporations operating globally.

7.3 Emerging Technologies and Data Protection Challenges

The rapid advancement of emerging technologies such as artificial intelligence, machine learning, blockchain, and big data analytics presents new challenges for data protection and corporate accountability. These technologies often rely on large-scale data processing, raising concerns about privacy, transparency, and algorithmic bias. For instance, AI systems may process personal data in ways that are difficult to explain, making it challenging to ensure compliance with principles such as purpose limitation and accountability. Additionally, technologies like blockchain, which involve decentralised data storage, may conflict with traditional data protection principles such as the right to erasure. These developments highlight the need for adaptive regulatory frameworks that can address technological innovations while safeguarding individual rights.

7.4 Role of Corporate Governance in Data Protection

Corporate governance plays a crucial role in ensuring effective data protection and accountability. Organisations are increasingly recognising data protection as a strategic issue that requires oversight at the highest levels of management. Board-level involvement, establishment of data protection committees, and integration of cybersecurity risk management into corporate governance frameworks are essential for ensuring compliance. Effective governance also involves fostering a culture of accountability, where employees are trained and aware of data protection obligations. By embedding data protection into corporate governance structures, organisations can enhance their ability to prevent data breaches and respond effectively to incidents.

7.5 Future Directions for India's Data Protection Regime

India's data protection framework is still evolving, and several measures can be adopted to strengthen its effectiveness in the future. These include the development of detailed rules and guidelines under the DPDP Act, strengthening the institutional capacity of regulatory authorities, and promoting awareness among corporations and individuals. There is also a need to align India's data protection standards with global frameworks to facilitate cross-border data flows and international cooperation. Additionally, the integration of technological solutions such as automated compliance tools and advanced cybersecurity systems can enhance enforcement and monitoring. By adopting a forward-looking approach, India can build a robust and resilient data protection regime that supports innovation while ensuring the protection of individual rights.

7.6 Conclusion

The comparative and forward-looking analysis highlights that while India has made significant

progress in establishing a comprehensive data protection framework, continuous adaptation is essential to address emerging challenges. Learning from global best practices, addressing gaps in cross-border data regulation, and integrating data protection into corporate governance will be critical for strengthening corporate accountability. As the digital economy continues to evolve, a dynamic and responsive regulatory framework will be necessary to ensure that data protection laws remain effective and relevant.

Bibliography

A. Statutes and Legislation

- Information Technology Act, 2000
- Digital Personal Data Protection Act, 2023
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- General Data Protection Regulation
- Personal Information Protection Law (PIPL), China
- Act on the Protection of Personal Information (APPI), Japan

B. Case Laws

- Justice K.S. Puttaswamy v. Union of India
- Shreya Singhal v. Union of India
- Google India Pvt. Ltd. v. Visaka Industries
- Avnish Bajaj v. State (NCT of Delhi)

C. Books

- Justice Yatindra Singh, *Cyber Laws* (Universal Law Publishing)
- Aparna Viswanathan, *Cyber Law: Indian and International Perspectives* (LexisNexis)
- Chris Reed & John Angel, *Computer Law* (Oxford University Press)
- Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer)

D. Journal Articles

- Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*
- Paul M. Schwartz, "Information Privacy in the Digital Age," *Harvard Law Review*
- Rahul Matthan, "Privacy and Data Protection in India," *Indian Journal of Law and Technology*
- Arghya Sengupta, "The Right to Privacy and Data Protection in India," *NUJS Law Review*

E. Reports and Government Documents

- Justice B.N. Srikrishna Committee Report on Data Protection (2018)
- Ministry of Electronics and Information Technology (MeitY), Government of India – DPDP Act Materials
- CERT-In Guidelines on Cyber Incident Reporting (2022)
- NITI Aayog, *Data Empowerment and Protection Architecture Report*

F. Websites and Online Sources

- Ministry of Electronics and Information Technology (MeitY): https://www.meity.gov.in
- CERT-In Official Website: https://www.cert-in.org.in
- European Commission – GDPR Portal: https://ec.europa.eu
- International Association of Privacy Professionals (IAPP): https://iapp.org
- PRS Legislative Research: https://prsindia.org

References

1. Information Technology Act, 2000, § 43A.
2. Digital Personal Data Protection Act, 2023.

3. Justice K.S. Puttaswamy v. Union of India.
4. Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*.
5. Justice B.N. Srikrishna Committee Report on Data Protection (2018).
6. General Data Protection Regulation.