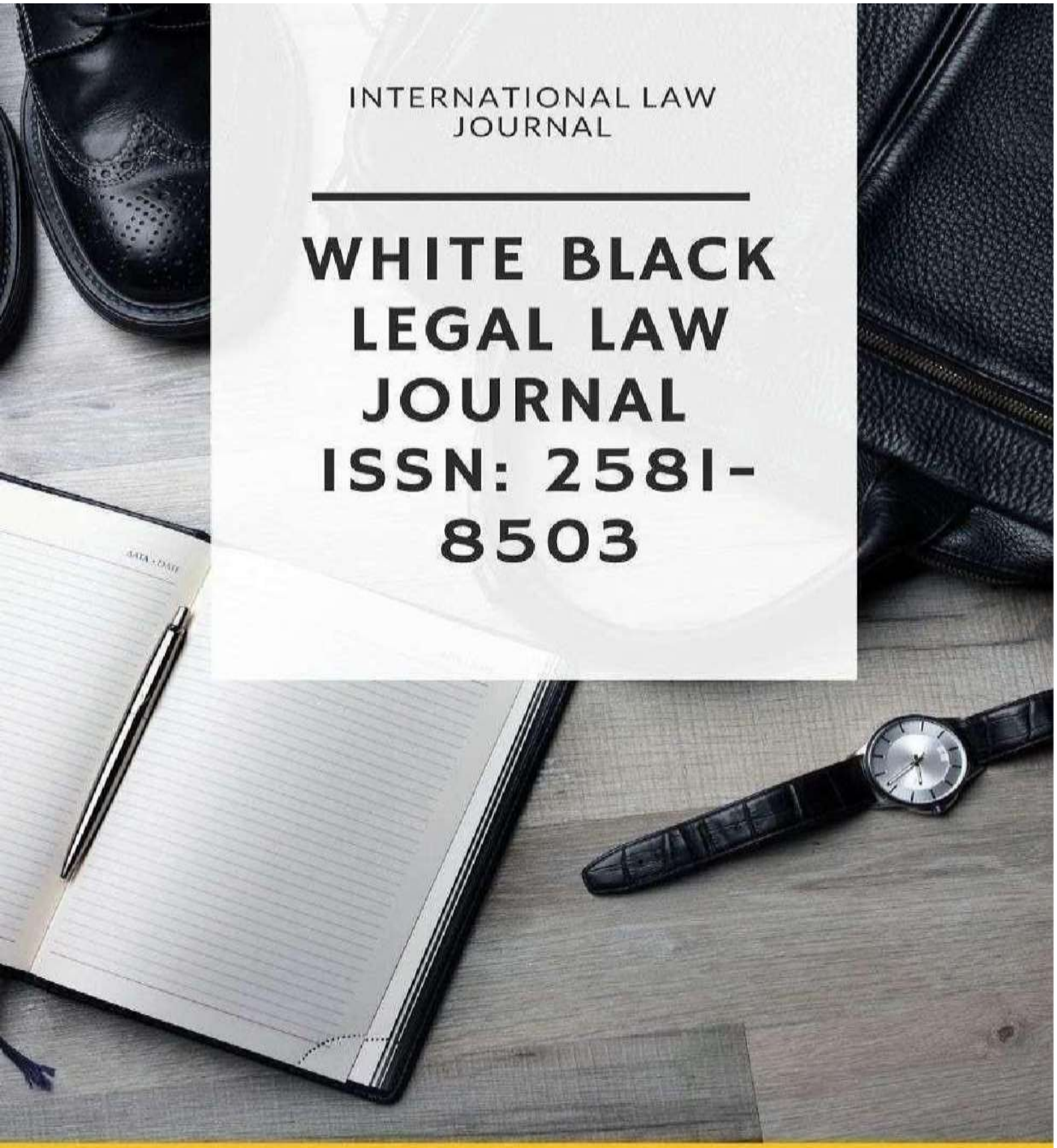

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

Data Protection And Corporate Accountability: A Study Of Legal Overlaps Between Company Law And Digital Regulation In India

Authored By - Aishwarya Verma

Abstract

Data protection is a crucial component of corporate governance since the quick development of digital technology has turned personal information into a valuable corporate asset. A major step toward controlling the processing of personal data has been taken in India with the passage of the Digital Personal Data Protection Act, 2023. However, it is impossible to comprehend corporate responsibility for data breaches without looking at how it interacts with the Companies Act of 2013 and the Information Technology Act of 2000. The intersection between company law and data protection law is critically examined in this essay, with an emphasis on director accountability and corporate liability. It contends that although the DPDP Act establishes a compliance-based structure with monetary penalties, there are gaps in enforcement because it does not include clear measures for individual accountability. The study's conclusion makes recommendations for changes that would improve accountability systems and incorporate data protection into corporate governance frameworks.

1. Introduction

Data is now a key resource for innovation, decision-making, and competitive advantage, and the emergence of the digital economy has completely changed how businesses operate. Businesses are depending more and more on the gathering and use of personal data, which raises serious issues about security breaches, abuse, and privacy. In Justice K.S. Puttaswamy v. Union of India (2017), the Supreme Court of India acknowledged the right to privacy as a basic right, which was a watershed in the evolution of data protection legislation in India.[1]The necessity for a thorough legal framework to protect personal data and control its processing by both state and non-state entities was highlighted by this historic ruling.

India responded to these advances by passing the Digital Personal Data Protection Act, 2023, which creates a formal framework for regulating digital personal data.[2] Although the Act offers a comprehensive framework for compliance, corporate responsibility for data protection cannot be restricted to legal requirements. The Companies Act of 2013's corporate governance

standards, which place an emphasis on responsibility and transparency and impose fiduciary duties on directors, must also be taken into consideration.[3]

In order to better understand how data protection law and company law intersect in India, this paper will focus on three research questions: first, whether corporate liability for data breaches is sufficiently addressed by the current legal framework; second, whether directors can be held accountable under current laws; and third, whether the overlap between various legal regimes creates gaps in enforcement. The study contends that the efficacy of the legal framework is compromised by the lack of a clear integration between corporate governance and data protection, even in spite of notable legislative advancements.

2. Evolution of Data Protection Law in India

2.1 Early Framework under the Information Technology Act, 2000

India mostly depended on the Information Technology Act, 2000, to handle concerns pertaining to electronic data and cybersecurity prior to the establishment of a specific data protection regime. Section 43A, which established the notion of corporate accountability for carelessness in upholding "reasonable security practices and procedures," was a key component of this framework.[4] This clause represented one of the first legal admissions that businesses handling private information must be accountable for its security. It essentially established a compensating process that allowed impacted parties to pursue damages in the event that a business neglected to put in place sufficient precautions. However, because it only applied to "body corporates" and in circumstances involving carelessness, the provision's scope was intrinsically limited, prohibiting strict liability and more comprehensive accountability procedures.

It was complemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which tried to add clarity in its operations by identifying sensitive personal data and stipulating some of the compliance areas such as consent, publication of privacy policies, and security measures such as ISO standards.[5] Though these rules were a significant move towards formalisation of the data protection practices, they had a number of structural flaws. Above all, they were limited in their applicability to a limited group of so-called sensitive personal data, thus not covering large volumes of personal data that were not confined to this term. Moreover, there were weak

enforcement mechanisms that were substantially based on adjudicating officers, making it inconsistent and a weak deterrent.

One of the strongest arguments against the IT Act framework was that it failed to introduce a rights-based approach to the protection of data. In contrast to the contemporary data protection regimes, it failed to acknowledge persons as entities with rights, and with a valid claim on their data. Rather, it considered the protection of data as a part of the contractual and tortious liability. Moreover, there was no specific regulatory or control body, and therefore, there was no central body where compliance was monitored, guidelines were issued, and penalties imposed uniformly. This piecemeal and responsive model finally proved to be insufficient in responding to the intricacies of the digital economy, giving way to a more unified legislative response.

2.2 Development of a detailed Framework: Digital Personal Data Protection Act, 2023

The introduction of the Digital Personal Data Protection Act, 2023, is a paradigm shift in how India manages its data, shifting towards a sectoral and fragmented system to a comprehensive and cohesive one. The Act provides a legal framework through which the processing of digital personal data is organized, and such principles as consent, purpose limitation, data minimization, and accountability are emphasized. Contrary to the previous IT Act framework, the DPDP Act is rights-based, with individuals being treated as the so-called data principals and guaranteed enforceable rights, such as the right to information access, the right to correct inaccuracies, and the right to have personal data erased.

The broadness of the application is one of the most characteristic aspects of the DPDP Act as it not only covers the information that is processed in India, but also those that are based in other countries, provided that they provide goods or services to people in the country. This extra territoriality indicates a conformity to international regulatory tendencies especially that of the European Union GDPR.[6] The Act also brings about the term of data fiduciaries, assigning the key responsibility to the parties that define the purpose and method of data processing. Such classification is important as it creates the fiduciary-like relationship between corporations and individuals, thus raising the level of the responsibility of the companies that process personal data.

The requirements under the DPDP Act are extensive and encompass the requirement of legal processing, adoption of security measures, breach reporting, and accountability. There is also

the establishment of a Data Protection Board which is provided by the Act to ensure enforcement and adjudication. Nevertheless, even along with such improvements, the Act takes a rather compliance-based and penalty driven approach, which relies on the financial fines on non-compliance. Although these penalties can be a deterring measure, they do not always guarantee substantive accountability, especially where there is nothing to deal with individual liability of directors or officers. It is an issue which makes the question whether the Act is effective in the field of systemic failures in the corporate governance systems.

3. Corporate Obligations under the Digital Personal Data Protection Act, 2023

3.1 Data Fiduciary and Corporate Responsibility

The notion of companies as data fiduciaries under the Digital Personal Data Protection Act, 2023, is a conceptual and legal change in the concept of corporate responsibility in data governance.[7] The data fiduciary refers to any entity that decides how and why personal data is processed, which practically places the majority of corporations, online platforms and service providers under the umbrella of this definition.[8] This name is not just a term, but has significant underlying substance, as it brings the logic of fiduciary relationships, historically existing in trust and corporate law and within agency relationships, to bear on the area of data protection.[9] In this way, the law increases the level of care that corporations should provide to others by ensuring that they do not just perform the duty that the statute stipulates but do it in the interests, rights, and autonomy of data principals.[10]

This fiduciary framing creates an ethical and governance aspect of data protection and makes it a technical compliance issue rather than an element of corporate responsibility. The corporations are supposed to operate in a legal, fair and transparent way so that the actions of data processing are not exploitative or excessive.[11] The fact that trust is valued is especially critical in the digital economy where people usually do not have bargaining power and access to the ways their data are processed. The awareness of this imbalance places a burden on corporations to reduce risks and alleviate harm, which is why the Act, even without specifically stating it, poses a responsibility on corporations to ensure their data protection is balanced with other ideas of corporate social responsibility and stakeholder governance.[12]

Further, there are also implications of fiduciary on internal corporate structures and decision-

making processes. It implies that data governance should be incorporated into the corporate strategy, and it should be governed on the highest management level.[13] It involves the internalization of policies, engagement of compliance officers and setting of accountability systems to enforce compliance with the law.[14] The designation of data fiduciaries, in this sense, can be seen as a compromise between digital regulation and corporate governance and a reminder of the necessity to approach accountability in a holistic manner.[15]

3.2 Key Obligations

The requirements of the data fiduciaries under the DPDP Act are broad and covered a preventive and compliance-based approach. The companies are obliged to get free, informed and specific consent of individuals to process their personal data with transparency and user control.[16] They should also keep the data accurate and comply with the principles of purpose limitation and data minimization, which should limit the unnecessary or excess data gathering. Moreover, businesses must adopt relevant technical and organizational security measures, such as encryption, access controls, and cybersecurity measures, to ensure that the data is not accessed or compromised by unauthorized individuals.[17]

Breach notification is one of the most significant provisions of the Act that requires companies to notify the regulatory authority and affected individuals in case of data breach. This promotes transparency and provides prompt remedial action. The Act also promotes the setting up of internal compliance systems, including grievance redressal systems and data protection policies, making data protection a continuous process in the organization. In general, these requirements prioritize risk management and proactive compliance, yet, their success mostly relies on corporate dedication and regulatory control.

3.3 Framework of Penalty and its limitations

The DPDP Act presents a strict payment system, which imposes serious financial fines in case of non-compliance to discourage non-compliance.[18] Although this puts significant emphasis on data protection, dependence on the use of monetary penalties is limited. Fines can be considered a cost that can be handled by large corporations making them less deterrent. More to the point, the Act fails to explicitly offer personal liability of directors or senior management which leaves a loophole in accountability.[19] Taking into consideration that most important decisions concerning data governance are taken at the managerial level, the lack of personal liability undermines the enforcement process and can be used to spread the responsibility

throughout the corporate hierarchy.

Moreover, the power of the penalty system will rely on whether the regulatory bodies can watch over adherence and administer penalties on a regular basis. In the absence of effective enforcement procedures and clear liability criteria, the structure is likely to be procedural instead of substantive. Thus, the penalty provisions are a step in the right direction, although they should be supplemented with greater connections to corporate governance and personal responsibility to make them effective.[20]

4. Corporate Governance under the Companies Act, 2013

4.1 Fiduciary Duties of Directors

Section 166 of the Companies Act, 2013 enshrines the fiduciary obligations of directors and provides a broad corporate governance framework.[21] In these responsibilities, the directors must act in good faith, with due care and skill and diligence and in the best interests of the company, its shareholders, employees and the community in general. The scope of these responsibilities renders them intrinsically adaptable and able to adjust to the new challenges, such as those that are appearing in the digital economy. When considering the issue of data protection, the responsibility of care and diligence gains special significance, since the directors are supposed to foresee the risks that can cause damage to the company, and address them. As data turns out to be a useful corporate asset, the inability to introduce proper data protection and cybersecurity can put companies at risk of financial losses, regulatory fines, and reputational loss. Therefore, directors might be required to make sure that systems, policies, and controls are in place to protect data.[22] This involves management of data governance systems, resource allocation to cybersecurity infrastructure, and ensuring adherence to the relevant data protection regulations. Therefore, despite the fact that there are no specific statutory requirements, fiduciary responsibilities may be applied to include data protection as a component of sound corporate governance.

4.2 Applicability to Data Protection

The Companies Act, 2013, does not explicitly mention data protection, but the provisions of the act are broad enough to be applied to data governance matters. The growing appreciation of data as a strategic and economic asset means that its safeguarding is tightly connected to the interests and sustainability of the company.[23] In this sense, any negligence or mismanagement

with regard to the protection of personal or sensitive data may constitute negligence or mismanagement, especially in cases where the negligence or mismanagement leads to regulatory fines or loss of stakeholder confidence. Directors who do not provide sufficient safeguards can thus be considered to have violated their fiduciary duties, particularly the duty of due diligence and acting in the best interests of the company.

The interpretation will be consistent with the current trends in conceptualizing corporate governance, which is progressively considers non-conventional risks like cybersecurity and data privacy. Nevertheless, the fact that data protection is not explicitly established in statutory law through the Companies Act leaves open the question of how far such a liability can go. The courts and regulators have not yet spelled out the scenarios in which a direct connection between breaches of fiduciary duty and data breaches can be made. This means that although the theoretical foundation of the director's liability is there, its applicability in practice is still doubtful. This loophole indicates that more explicit legal guidelines or judicial precedent are necessary to fill the gap between the law of the company and digital regulation.[24]

4.3 Corporate Accountability and Risk Management.

The Companies Act, 2013, lays a lot of stress on corporate accountability by introducing various mechanisms that include internal controls, audit requirements, and risk management systems, which are directly applicable to data protection.[25] Firms are supposed to detect, evaluate, and manage risks that may impact their operations, such as technological and cybersecurity threats. Data breaches and cyberattacks are significant threats in the digital age that may sabotage business activities and destroy trust among stakeholders. In line with this, risk management strategies should be well-developed to mitigate risks, and this should encompass data protection policies, data storage, access control, response to incidents, and monitoring of compliance.

Board level control is important in maintaining that such risks have been properly managed. Directors should have direct involvement in risk management procedures, read cybersecurity and data protection reports, and make sure that proper governance frameworks exist. This can be through the formation of special committees, the selection of data protection or data compliance officers, and the incorporation of data protection into enterprise risk management systems.[26] These actions indicate a transition to the perspective of considering data protection as a management problem instead of a more technical or operational one.

But, practically, most corporations still look at data protection as a regulatory requirement as opposed to an element of corporate governance. Such a narrow focus can lead to insufficient investment in cybersecurity infrastructure and a lack of board-level attention. As a result, even though there are governance frameworks in the Companies Act, the incorporation of data protection in the frameworks is mixed. This integration needs to be reinforced so that corporate responsibility can be applied to personal data protection to match the requirements of the digital economy with company law.[27]

5. Interplay between Data Protection Law and Company Law

The connection between the Digital Personal Data Protection Act, 2023 and the Companies Act, 2013 depicts a meeting point between two different yet increasingly related concepts of regulation, the former based on compliance-based digital regulation, and the latter on principle-based corporate governance. The DPDP Act creates a comprehensive statutory regulation that creates certain duties on the entities that are categorized as data fiduciaries with a strong emphasis on lawful processing, consent, security, as well as breach disclosure. Conversely, the Companies Act is a wider level law as it focuses on fiduciary duties, accountability, transparency, and responsible management in its governance principles. A combination of these structures could develop a comprehensive system of corporate responsibility where compliance of the organization and managerial accountability are tackled.

Nevertheless, regardless of this potential complementary nature, lack of explicit statutory integration between the two regimes leaves huge gaps. The DPDP Act is largely related to corporate liability, which is mainly expressed in financial fines on the entity; the Companies Act is concerned with the behavior and responsibilities of directors without mentioning data protection in particular. This disconnect leads to an inconsistent approach to accountability in that a company could be fined in the DPDP Act over a data breach, but the individuals involved in the oversight and decision-making might not face the consequences of the company law. Consequently, accountability becomes more or less decentralized throughout the corporate system, undermining the entire enforcement process.

One of the main concerns of such a deficit in integration is the ambiguity of the issue of director liability in the cases of data breach. Although, in theory, a failure to take reasonable data

protection practices can be viewed as a violation of fiduciary duty under Section 166 of the Companies Act, this interpretation is not formally codified in the legislation, nor has a strong basis in case law. This leaves uncertainty on the conditions of personal liability of the directors, and thus enforcement is inconsistent and unpredictable. Furthermore, the lack of definite legal norms to associate the failure of data governance with the violation of fiduciary duties restricts the capacity of regulators and courts to hold accountable effectively.

The interaction between the two legal frameworks also draws out a more general conceptual question as to what corporate responsibility is in the digital age. The DPDP Act views data protection as a regulatory compliance issue, whereas the Companies Act offers an opportunity to introduce data protection to corporate governance. To close this divide, it is essential to view data protection not as a technical or compliance problem but as an inseparable part of governance that the directors should take into account as a part of their responsibility. In the absence of such integration, the legal framework may continue to be compartmentalized, thus not responding to the systemic data protection issues faced by corporations in the contemporary society.

6. Legal and Practical Challenges

The presence of several legal systems that regulate data protection and corporate practices in India presents a set of various legal and practical issues, which complicate the successful exercise of corporate accountability. Among the most crucial issues is the lack of clarity in liability establishment, especially where a data breach is concerned. The DPDP Act subject data fiduciaries to a duty and penalties in the event of non-compliance, but does not explicitly specify the standard of care expected or the situations in which a fiduciary will be liable.[28] Likewise, the Companies Act does not specifically speak on the data protection and the duty of directors, which leaves a lot to be desired. Such ambiguity places both corporations and regulators in a state of confusion, and it is hard to have a similar standard of accountability.[29] The other significant issue is the lack of unity in the legal system, which consists not only of the DPDP Act and the Companies Act but also of the Information Technology Act, 2000, and other industry-specific regulations.[30] The overlap of these laws may result in duplication of requirements, conflicting requirements, and regulatory confusion. As an example, different companies can be expected to adhere to various standards of reporting and security, and they have various thresholds and processes. This fragmentation adds to compliance costs and

administrative burdens, especially to smaller companies that might not have the resources to cope with intricate regulatory demands. It also opens possibilities of regulatory arbitrage whereby, businesses are able to take advantage of the discrepancies between regulations to reduce their liability.

Another serious challenge is enforcement because the success of the legal framework relies on the ability and coordination of regulatory bodies. The DPDP Act envisages the creation of a Data Protection Board, which will have its efficacy determined by such factors as institutional independence, technical knowledge and enforcement authority. Without effective regulatory control, compliance can be superficial, with firms paying attention to the formal compliance with requirements as opposed to the actual data protection practice. Moreover, the absence of cooperation between various regulatory authorities, including those that may regulate corporate governance and digital regulation, may lead to enforcement and accountability loopholes.[31]

The introduction of data protection laws is also complicated by technological issues. The blistering development of digital technologies, such as artificial intelligence, big data analytics, and cloud computing, has added complexity to the data processing process and increased the risk of breaches.[32] The cybersecurity threats keep evolving and necessitate ever-investment in hi-tech security systems and human resources. Nevertheless, most companies, especially small organizations, might not be in a position to match such developments due to resource constraints and lack of professionalism. This introduces a disconnect between the legal requirements and the actual abilities, and adhering to it becomes harder.

Additionally, there is the complexity of the global character of data flows. The extraterritorial scope of the DPDP Act implies that the companies, which operate in several jurisdictions, have to deal with numerous regulatory frameworks with their corresponding requirements and standards. This has the potential to cause conflicts of law especially in issues of localization of data, cross-border transfer of data and privacy standards. Compliance in such a dynamic and complex environment should not only be ensured through legal clarity, but also through strong institutional frameworks and international cooperation.

Apart from these structural issues, the issue also has an organizational and cultural component. Data protection is still seen by many businesses as a compliance need rather than a strategic objective, which leads to insufficient board attention. Because compliance becomes a box-

ticking process rather than a meaningful commitment to data protection, this approach compromises the efficacy of legal frameworks. A change in business culture that places more of a focus on ethical data governance, accountability, and transparency is necessary to address this issue.[33]

7. Critical Analysis

The critical analysis of the Indian legal system of data protection and corporate responsibility shows that there are a number of structural and conceptual gaps that restrict its overall efficiency. The excessive use of financial fines as the main enforcement tool in the Digital Personal Data Protection Act, 2023, is one of the most noticeable problems.[34] Financial sanctions can theoretically be a deterrent; however, in reality, this is not always the case, especially when dealing with a large corporation that has huge financial capabilities. These organizations can absorb fines as operational expenses, thus diluting the deterrent impact and undermining the regulatory goal of deterring data breaches.

The second major limitation is that there are no clear terms on the issue of personal liability of directors and senior management. Generally, the data protection failure is not clearly stipulated as a duty of directors under the Companies Act, 2013, although it imposes the fiduciary duties on directors.[35] This creates a gap between corporate responsibility and personal responsibility so that decision-makers can escape the repercussions of any data governance failures. Since most data breaches are caused by weak oversight, poor risk management, or negligence on the part of the management, the lack of personal liability will weaken the efficiency of the law system in ensuring that the causes of such failures are addressed.

Also, the disjointed quality of the regulatory structure is a significant problem. The overlapping nature of various legal tools, such as the DPDP Act, the Companies Act, and the Information Technology Act, 2000, gives rise to complexities in obligation, inconsistencies, and compliance.[36] This division not only augments the regulatory load of corporations but also leaves the existence of unpredictability as to which standards and enforcement mechanisms apply. Consequently, the legal framework is incoherent and does not offer a common strategy on data protection and corporate responsibility.

Moreover, the conceptual restriction of the treatment of data protection within the current

framework is wider. It is typically dealt with as a compliance matter and not an essential aspect of corporate governance. This is a very subjective view, which restricts the concept of incorporating data protection in strategic decision-making and makes it less significant in corporate structures. As a result, formal compliance has become the major focus of many organizations, with the result that there can be differences between law and practice.[37]

8. Recommendations

To overcome the challenges, a more integrated data protection and corporate governance approach should be embraced. One of the reforms would be to clearly connect the data protection requirement with the fiduciary duty of the directors under the Companies Act, 2013, such that the individual directors would be held accountable on failure to take proper care of the data governance. Moreover, aligning the Digital Personal Data Protection Act, 2023, with the current legislation, e.g., the Information Technology Act, 2000, would assist in lessening the fragmentation and offer more precise compliance criteria. Enhancing enforcement procedures and encouraging board-level data protection control can also help to make sure that the legal requirements are properly enforced into practice.

9. Conclusion

The interaction between data protection law and the law of companies in India is an extremely significant field in the development of the law in the digital era, indicating the increasing significance of data as a company resource, and the necessity of effective mechanisms to guarantee its security. The Digital Personal Data Protection Act, 2023, offers a framework to regulate data processing and introduce a system of compliance requirements on corporations. But this has limited its success inasmuch as it does not have a clear integration with corporate governance principles under the Companies Act, 2013, especially in regard to director accountability. To close this gap, it is necessary to have a holistic approach that integrates regulatory compliance with governance norms, so that not only corporations are accountable to data protection failures, but also their decision-makers. This is not only through reinforcing the law but also the creation of a culture of responsibility and ethical behavior in corporate systems. As India moves in the direction of developing its data protection regime, it will be important to streamline the digital regulation with the company law, in order to develop an integrated and effective framework that would balance the interests of the business, individual, and society in the digital age.

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[2] Digital Personal Data Protection Act, 2023.
[3] Companies Act, 2013, § 166.
[4] Information Technology Act, 2000, § 43A.
[5] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
[6] General Data Protection Regulation, Regulation (EU) 2016/679.
[7] Digital Personal Data Protection Act, 2023.
[8] Id. § 2(i) (definition of Data Fiduciary).
[9] Tamar Frankel, *Fiduciary Law* 1–5 (Oxford Univ. Press 2011).
[10] DPDP Act, 2023, supra note 1.
[11] Id.
[12] Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019).
[13] OECD, *Corporate Governance and Data Protection* (2020).
[14] Companies Act, 2013, § 166.
[15] DPDP Act, 2023, supra note 1.
[16] Id.
[17] Id. § 6 (Consent).
[18] Digital Personal Data Protection Act, 2023, Ch. VIII.
[19] Id.
[20] Id.
[21] Companies Act, 2013, § 166.
[22] Id.
[23] OECD, *Corporate Governance and Data Protection* (2020).
[24] Id.
[25] Companies Act, 2013, supra note 4.
[26] Id.
[27] Ministry of Corporate Affairs, *Report on Corporate Governance Practices in India* (2021).
[28] Digital Personal Data Protection Act, 2023.
[29] Companies Act, 2013, § 166.
[30] Information Technology Act, 2000.
[31] Ministry of Electronics & IT, Govt. of India, *DPDP Act Explanatory Framework* (2023).
[32] OECD, *Digital Security Risk Management* (2021).
[33] World Bank, *Data Governance and Corporate Accountability Report* (2022).
[34] Digital Personal Data Protection Act, 2023.
[35] Companies Act, 2013, § 166.
[36] Information Technology Act, 2000.
[37] OECD, *Corporate Governance and Data Protection* (2020).