RETHINKING CORPORATE GOVERNANCE UNDER THE DPDP FRAMEWORK: DATA BREACH LIABILITY AND BOARD OVERSIGHT OF ARTIFICIAL INTELLIGENCE DEPLOYMENT IN PRIVATE COMPANIES

Adv. Thushara Menon, LL.M (Commercial Law),
Bharata Mata School of Legal Studies, Ernakulam, Kerala

ABSTRACT

The rapid adoption of Artificial Intelligence (AI) by private companies has transformed the manner in which personal data is connected, processed, analysed and utilised for commercial purposes**.** While AI systems can improve efficiency and decision-making, their increasing reliance on personal data also creates significant concerns relating to data security, accountability and corporate risk management. The Digital Personal Data Protection Act, 2023 (DPDP Act) provides an important statutory framework for regulating the processing of digital personal data in India and places significant responsibilities upon Data Fiduciaries, including obligations relating to security safeguards and personal data breaches. These obligations assume greater importance where companies deploy AI systems or rely on external AI service providers for processing personal data.

This paper examines data breach liability and board oversight in private companies through the emerging intersection of corporate governance, data protection and AI deployment. It analyses the responsibilities imposed upon Data Fiduciaries under the DPDP framework and considers their relationship with existing duties of directors under the Companies Act, 2013. Particular attention is given to the distinction between the technical responsibility of management and processors and the broader governance responsibility of boards to identify and oversee material data-related risks. The paper argues that although the DPDP Act does not establish a universal statutory requirement for boards to supervise every AI system or conduct algorithmic audits, companies should integrate significant data-protection and AI-related risks into their existing corporate governance and risk-management structures. Such an approach can strengthen accountability while avoiding an unwarranted expansion of statutory obligations beyond what the law presently provides.

Keywords: Digital Personal Data Protection Act, 2023; Corporate Governance; Artificial Intelligence; Data Breach; Board Oversight; Data Fiduciary.

1. Introduction

The rapid expansion of digital technologies has altered the manner in which private companies conduct business, interact with consumers and manage organisational processes. Among the technologies that have produced the most significant changes is artificial intelligence (AI). Private companies increasingly employ AI-enabled systems for activities such as customer profiling, targeted advertising, recruitment, fraud detection, credit assessment, recommendation systems and automated decision-making. Many of these applications depend upon the collection and processing of personal data. Consequently, the deployment of AI has transformed data protection from a predominantly technical or compliance-oriented concern into an issue that increasingly intersects with corporate governance.[1]

The governance implications become particularly significant when the use of AI involves large volumes of personal data or reliance upon external technology providers. A company may obtain an AI system from a third-party provider, integrate it into its internal operations and use it to process information relating to individuals without the board being directly involved in the technical operation of the system. Nevertheless, a failure in the security or governance of such processing may expose the company to legal, financial and reputational consequences. The question therefore arises as to where responsibility should lie when data-processing activities are increasingly complex and technologically dependent. While the technical management of information-security systems may remain with specialised personnel and service providers, significant data-related risks cannot necessarily be treated as matters outside the broader responsibilities of corporate governance.

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) represents an important development in India's data-protection framework. The Act establishes a statutory framework for the processing of digital personal data and places primary responsibility upon the Data Fiduciary for ensuring compliance with its obligations. The statutory framework addresses matters including lawful processing, notice, consent, security safeguards, notification of personal data breaches, erasure of personal data and grievance redressal. Significantly, the Act also imposes additional obligations upon Significant Data Fiduciaries, including the appointment of a Data Protection Officer, appointment of an independent data auditor and periodic data protection impact assessments and audits. These provisions demonstrate that data

[1] See NITI Aayog, *Responsible AI: A Report on Principles for Responsible AI*, NITI Aayog (2021), https://www.niti.gov.in/sites/default/files/2021-02/Part1-Responsible-AI-1202.pdf.

protection is not confined exclusively to technical security but can also involve organisational structures of accountability.[2]

The relationship between data protection and corporate governance becomes more evident when the DPDP framework is considered alongside the Companies Act, 2013. Section 166 of the Companies Act sets out statutory duties of directors, including the duty to act in good faith, exercise due and reasonable care, skill and diligence, and exercise independent judgment. Section 177 further recognises the role of the Audit Committee in evaluating internal financial controls and risk management systems in companies to which that provision applies.[3] These provisions do not expressly create a specific statutory duty upon directors to supervise AI deployment or data protection in every private company. However, they provide a broader corporate-governance context within which material technological and data-related risks may require appropriate oversight.

The constitutional dimension of data protection also provides an important foundation for this discussion. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court of India recognised the right to privacy as a constitutionally protected right under Article 21 and the broader guarantees of Part III of the Constitution.[4] The judgment specifically recognised informational privacy as an aspect of individual privacy. Although *Puttaswamy* was not concerned with AI deployment or the DPDP Act, its recognition of informational privacy provides an important constitutional backdrop for understanding the protection of personal data in an increasingly data-driven economy.

The emergence of AI therefore presents a more complex governance environment. AI systems may involve extensive data collection, automated processing and dependence on third-party processors, creating risks that may not be adequately addressed through conventional compliance mechanisms alone. At the same time, it would be legally inaccurate to treat the DPDP Act as a comprehensive AI-governance statute or to assume that it imposes a general obligation upon every private company to conduct algorithmic audits. The Act is principally concerned with the processing of digital personal data, and its application to AI depends substantially upon whether and how personal data is processed within a particular activity.[5]

This distinction is important because corporate governance should not be expanded merely by

[2] Digital Personal Data Protection Act, No. 22 of 2023, § 8(1), (4)–(6), India Code (2023)
[3] Companies Act, No. 18 of 2013, §§ 166(2)–(3), 177(1), (4)(vii), India Code (2013).
[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[5] Digital Personal Data Protection Act, No. 22 of 2023, §§ 2–4, India Code (2023).

attributing every technological risk to the board. The more appropriate question is whether significant data-protection risks arising from corporate AI deployment should form part of the board's broader oversight of organisational risk. The issue is particularly relevant where a data breach can result not only from an internal security failure but also from vulnerabilities associated with third-party Data Processors, inadequate access controls or inappropriate technological practices. The DPDP framework places responsibility upon the Data Fiduciary even where processing is undertaken on its behalf by a Data Processor, thereby making organisational accountability an important component of data protection.[6]

Against this background, this paper examines the relationship between data breach liability, corporate governance and board oversight in private companies deploying AI systems. It seeks to determine how the DPDP framework can be situated within existing corporate-governance principles without attributing obligations to directors that the statute does not expressly impose. The paper argues that the increasing use of AI makes data protection a material corporate governance concern, particularly where personal data is processed at scale or where significant risks arise from third-party technological infrastructure. However, effective governance requires a distinction between statutory compliance obligations, management-level technical responsibilities and the board's broader responsibility to oversee material organisational risks.

The paper therefore adopts a focused approach. Rather than treating AI governance as an independent and comprehensive field, it examines AI deployment principally as a contemporary context in which data-protection and corporate-governance risks increasingly converge. This approach enables the DPDP framework to be assessed not merely as a data protection statute but also in terms of its implications for corporate accountability, risk oversight and responsible technological decision-making within private companies.

2. Objectives and Research Question

2.1 Objectives of the Study

The primary objective of this paper is to examine the relationship between data protection, corporate governance and the deployment of artificial intelligence by private companies within the framework established by the Digital Personal Data Protection Act, 2023. The study particularly focuses on the extent to which data-related risks arising from AI deployment

[6] Id. § 8(1)–(2).

should be treated as matters of corporate governance rather than solely as technical or operational concerns.

The paper seeks to examine the obligations of Data Fiduciaries concerning the security of personal data and personal data breaches, with particular attention to the responsibility of companies where processing is undertaken through third-party Data Processors. It further seeks to analyse how these obligations may affect the internal allocation of responsibility between the board, senior management, technology personnel and external service providers.

A further objective is to examine whether existing corporate-governance principles under the Companies Act, 2013 provide an adequate basis for board-level oversight of significant dataprotection risks associated with AI deployment. The study does not assume that the Companies Act or the DPDP Act imposes a general duty upon every private company to subject its AI systems to board-level supervision. Instead, it considers whether existing duties relating to care, diligence and risk oversight can provide a governance basis for addressing material data-related risks.

The paper also seeks to identify the limits of the DPDP framework in relation to AI. In particular, it examines whether the Act should be understood as indirectly regulating certain consequences of AI deployment where personal data is processed, rather than as a comprehensive statute governing AI systems themselves. This distinction is important to avoid attributing regulatory requirements to the DPDP Act that are not expressly contained in it.

Finally, the paper proposes a governance-oriented approach through which private companies can integrate significant data-protection and AI-related risks into existing corporate risk management structures while maintaining a clear distinction between statutory obligations and voluntary governance practices.

2.2 Research Questions

The study addresses the following research questions:

1. How does the Digital Personal Data Protection Act, 2023 regulate the responsibility of private companies for personal data security and data breaches, particularly where processing is undertaken through Data Processors?

2. To what extent can data-protection risks arising from the deployment of AI systems be treated as a matter of corporate governance and board oversight?

3. How do the duties of directors and existing corporate-governance mechanisms under the Companies Act, 2013 interact with the data-protection responsibilities established under the DPDP framework?

4. Does the DPDP framework provide an adequate basis for addressing the governance risks associated with AI-driven processing of personal data, or are additional organisational mechanisms required?

5. What governance measures can private companies adopt to strengthen board-level oversight of material data-protection risks associated with AI deployment without creating statutory obligations that are not presently recognised by law?

3. Legal Framework

3.1 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 ("DPDP Act") constitutes the principal statutory framework governing the processing of digital personal data in India. The Act adopts the concepts of the "Data Principal," whose personal data is processed, and the "Data Fiduciary," which determines the purpose and means of processing personal data.[7] This distinction is significant for private companies because the entity determining why and how personal data is processed will ordinarily bear the principal statutory responsibility for compliance with the Act.

The Act applies to the processing of digital personal data within India where the personal data is collected from Data Principals in digital form or collected in non-digital form and subsequently digitised. It also extends to processing outside India where such processing is in connection with offering goods or services to Data Principals within India.[8] The scope of the Act is therefore capable of covering data-processing activities undertaken by private companies in connection with their commercial operations, including activities involving digital

[7] Digital Personal Data Protection Act, No. 22 of 2023, 2(i), (j), India Code (2023)
[8] Id. § 3.

technologies and AI systems, where the statutory conditions for application are satisfied.

Section 4 establishes the basic requirement for lawful processing by providing that a person may process personal data only in accordance with the provisions of the Act and for a lawful purpose. Such processing may be based on the consent of the Data Principal or for certain legitimate uses recognised by the Act.[9] The statutory framework therefore places limits on the manner in which companies may collect and process personal data rather than leaving such processing exclusively to contractual or technological arrangements.

Of particular relevance to the present study is section 8, which sets out the general obligations of a Data Fiduciary. Section 8(1) makes the Data Fiduciary responsible for compliance with the provisions of the Act and the rules made thereunder in respect of processing undertaken by it or on its behalf by a Data Processor. This provision assumes particular importance where companies use external technology providers, cloud infrastructure or other third-party services in connection with AI-enabled processing. Outsourcing the processing activity does not, by itself, remove the Data Fiduciary's statutory responsibility.[10]

Section 8 further requires a Data Fiduciary to implement appropriate technical and organisational measures to ensure effective observance of the provisions of the Act and to take reasonable security safeguards to prevent personal data breaches.[11] Where a personal data breach occurs, the Data Fiduciary is required to give intimation of the breach to the Data Protection Board of India and to each affected Data Principal in the prescribed manner and form.[12] These provisions establish data security and breach response as continuing organisational responsibilities rather than matters arising only after an incident has occurred.

The Act also establishes additional obligations for entities designated as Significant Data Fiduciaries. Under § 10, the Central Government may notify a Data Fiduciary or class of Data Fiduciaries as a Significant Data Fiduciary on the basis of factors including the volume and sensitivity of personal data processed, the risk to the sovereignty and integrity of India, the risk to electoral democracy, security of the State, public order and other prescribed considerations.[13] Significant Data Fiduciaries are subject to enhanced compliance requirements, including the

[9] Id. § 4.
[10] Id. § 8(1)–(2)
[11] Id. § 8(4)–(5)
[12] Id. § 8(6)
[13] Id. § 10(1)

appointment of a Data Protection Officer, the appointment of an independent data auditor and the undertaking of periodic Data Protection Impact Assessments and audits.[14]

The DPDP Act also provides for substantial financial penalties for specified breaches. Under § 33 read with the Schedule, failure to take reasonable security safeguards to prevent a personal data breach may attract a penalty extending to ₹250 crore, while failure to notify a personal data breach in accordance with the Act and rules may attract a penalty extending to ₹200 crore.[15] The potential scale of these penalties reinforces the importance of treating data protection as a significant organisational risk, although the statutory penalty is imposed through the mechanism prescribed by the Act and is not automatically equivalent to liability of individual directors.

3.2 Digital Personal Data Protection Rules, 2025

The Digital Personal Data Protection Rules, 2025 ("DPDP Rules") provide the subordinate regulatory framework required for the implementation of the DPDP Act. The Rules were notified by the Central Government on November 13, 2025.[16] Their significance lies not merely in supplementing the substantive obligations contained in the Act but also in prescribing the manner in which several obligations are to be operationalised.

The Rules adopt a phased commencement structure. Rules 1, 2 and 17 to 21 came into force upon publication, while Rule 4 is to come into force one year after publication. Rules 3, 5 to 16 and 22 to 23 are to come into force eighteen months after publication.[17] The phased commencement is legally significant for the present paper because the DPDP framework should not be treated as though every substantive obligation became operational immediately upon notification.

Rule 6 is particularly relevant to data security. It requires Data Fiduciaries to implement reasonable security safeguards to prevent personal data breaches and identifies measures including appropriate security practices such as encryption, masking or tokenisation, access controls, logging and monitoring, and periodic review of relevant measures.[18] These

[14] Id. § 10(2)
[15] Id. § 33, sched., Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023)
[16] Digital Personal Data Protection Rules, 2025, Gazette of India, G.S.R. 846(E) (Nov. 13, 2025)
[17] Id. r. 1(2)–(4)
[18] Id. r. 6.

requirements give greater operational substance to the security-safeguard obligation contained in section 8(5) of the Act.

The Rules also provide the procedural framework for notification of personal data breaches.

The prescribed requirements are important because the statutory obligation to notify a breach must operate through a defined process capable of providing information to both the Data Protection Board and affected Data Principals.[19] Accordingly, corporate preparedness for a data breach cannot be limited to preventing unauthorised access; it must also include an appropriate response and notification mechanism.

3.3 Companies Act, 2013 and Corporate Governance

The Companies Act, 2013 provides the broader corporate-governance framework within which the responsibilities of directors and specified corporate committees are exercised. Section 166 imposes statutory duties upon directors, including the duty to act in good faith in order to promote the objects of the company for the benefit of its members as a whole, and to act in the best interests of the company, its employees, shareholders, the community and for the protection of the environment. Directors are also required to exercise their duties with due and reasonable care, skill and diligence and to exercise independent judgment.[20]

These provisions do not expressly refer to personal-data protection or AI deployment. Nevertheless, the requirement of due care, skill and diligence provides a relevant governance principle when directors are required to oversee material risks arising from the company's operations. The relevance of section 166 to data protection must therefore be understood as part of the broader duties of directors rather than as creating an independent statutory data protection obligation.

Section 177 further provides for the constitution of an Audit Committee in every listed public company and such other classes of companies as may be prescribed.[21] Among the functions assigned to the Audit Committee is the evaluation of internal financial controls and risk management systems. The provision demonstrates that corporate governance under Indian company law already recognises the importance of structured oversight of organisational

[19] Id. r. 7.
[20] Companies Act, No. 18 of 2013, § 166(2)–(3), India Code (2013)
[21] Id. § 177(1)

risks.[22] However, its application should not be overstated: the provision does not expressly require an Audit Committee to supervise AI systems or DPDP compliance in every private company.

3.4 Constitutional Privacy and the Data-Protection Framework

The statutory framework for personal-data protection must also be understood against the constitutional recognition of privacy. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge Bench of the Supreme Court unanimously recognised the right to privacy as a constitutionally protected right.[23] The judgment recognised informational privacy as an aspect of privacy and observed that individuals have an interest in controlling the dissemination of personal information.[24]

The constitutional recognition of informational privacy provides an important normative foundation for contemporary data-protection regulation. At the same time, the DPDP Act operates as a statutory framework governing specified forms of personal-data processing. The constitutional right to privacy and the statutory obligations under the DPDP Act should therefore not be treated as identical sources of legal obligation. The former provides the constitutional context within which privacy interests are understood, while the latter establishes specific statutory duties, rights and enforcement mechanisms.

Taken together, the DPDP Act, the DPDP Rules, the Companies Act and the constitutional privacy framework provide the legal foundation for examining the governance implications of AI-enabled personal-data processing. The central issue is not whether these instruments expressly create a comprehensive regime of AI governance. Rather, it is whether their existing principles and obligations are sufficient to ensure that material data-protection risks associated with AI deployment receive appropriate corporate oversight.

4. Analysis of the Topic

4.1 Data Breach Liability as a Corporate Governance Concern

Data breaches have traditionally been approached by companies as information-security

[22] Id. § 177(4)(vii)
[23] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[24] Id

incidents requiring a technical response. The DPDP framework, however, makes it difficult to view a serious breach solely as a matter for the information-technology department. Section 8 places responsibility for compliance upon the Data Fiduciary and requires the implementation of appropriate technical and organisational measures and reasonable security safeguards to prevent personal data breaches.[25] The statutory responsibility therefore attaches to the organisation that determines the purpose and means of processing, even where the actual processing is carried out through another entity.

This has important consequences for corporate governance. A significant data breach can affect a company's financial position, contractual relationships, customer confidence and reputation. Where the company processes substantial quantities of personal data, a failure to establish adequate safeguards may therefore constitute a material organisational risk. The potential penalties under the DPDP Act reinforce this concern. The Schedule to the Act provides for penalties extending up to ₹250 crore for failure to take reasonable security safeguards to prevent a personal data breach and up to ₹200 crore for failure to notify a personal data breach as required by the Act.[26]The existence of these statutory consequences strengthens the argument that data protection should be incorporated into broader corporate risk-management structures rather than treated as an isolated technical function.

This does not mean that every data breach automatically establishes personal liability on the part of directors. The DPDP Act primarily places the relevant obligations upon the Data Fiduciary, and the statutory penalty framework operates against the person or entity responsible under the Act. The question of board oversight is therefore different from the question of individual liability. Board oversight concerns whether significant risks are appropriately identified, evaluated and addressed within the company's governance structure; it should not be confused with automatic attribution of every operational failure to individual directors.

The distinction is particularly important for private companies. Not every private company is subject to the same corporate-governance mechanisms under the Companies Act, and not every company processing personal data will qualify as a Significant Data Fiduciary. Consequently, a governance model that imposes identical board-level procedures upon all private companies would not accurately reflect the differentiated structure of the statutory framework. The

[25] Digital Personal Data Protection Act, No. 22 of 2023, § 8(1), (4)–(5), India Code (2023)
[26] Id. § 33, sched

appropriate level of oversight should instead correspond to the nature, scale and significance of the data-processing activities and the risks associated with them.

4.2 Responsibility of the Data Fiduciary Where AI Processing is Outsourced

The use of AI frequently involves multiple participants. A private company may develop an AI system internally, purchase an AI-enabled service from another company or use an external provider to process data through an AI model. This creates a potential separation between the entity that decides the purpose of processing and the entity that technically performs the processing.

The DPDP Act addresses this issue through the relationship between the Data Fiduciary and Data Processor. Section 8(1) provides that the Data Fiduciary remains responsible for compliance in respect of processing undertaken by it or on its behalf by a Data Processor. Section 8(2) further provides that a Data Fiduciary may engage a Data Processor for undertaking processing activities on its behalf only under a valid contract.[27] The provisions are particularly relevant to AI deployment because companies may rely upon external cloud providers, software vendors, analytics platforms or AI service providers in processing personal data.

The outsourcing of processing therefore cannot be treated as a complete transfer of legal responsibility. A company cannot simply argue that a breach resulted from the technical conduct of its external provider and that the matter consequently falls outside the company's governance responsibilities. The statutory framework places the Data Fiduciary in a position of continuing responsibility for processing undertaken on its behalf.

From a corporate-governance perspective, this creates a need for companies to understand the data-processing functions performed by external AI providers and the risks associated with those arrangements. This may include identifying what personal data is being processed, determining the purpose for which it is being processed, assessing the contractual arrangements with the provider and ensuring that appropriate security measures are incorporated into the relationship. The board need not perform the technical assessment itself. Its role is more appropriately understood as ensuring that the organisation has an effective system through

[27] Id. § 8(1)–(2)

which material risks are identified and addressed.

4.3 Board Oversight and the Duties of Directors

The Companies Act provides an important basis for considering the role of directors in relation to emerging technological risks. Section 166(3) requires directors to exercise their duties with due and reasonable care, skill and diligence and to exercise independent judgment.[28] The provision does not expressly refer to cybersecurity, personal data or AI. Nevertheless, the broad requirement of due care and diligence may become relevant where a company's operations expose it to significant and foreseeable risks.

A company's board is not expected to possess the technical expertise necessary to examine the architecture of every AI model or security system. Corporate governance does not require directors to become information-technology specialists. Rather, effective oversight requires directors to obtain sufficient information to understand material risks and to ensure that appropriate systems of management and internal control exist to address those risks.

This distinction becomes especially important in the context of AI. The technical complexity of AI systems may make it difficult for non-specialist decision-makers to identify the consequences of particular processing practices. If personal data is being processed through an AI system, however, the board cannot reasonably treat the matter as entirely disconnected from the company's legal and operational risks. The appropriate governance response is therefore not necessarily direct technical supervision but informed oversight supported by competent management, compliance personnel and technical specialists.

The Companies Act's provisions concerning risk management and internal controls provide a further basis for this approach. Section 177(4)(vii) assigns to the Audit Committee, in companies to which Section 177 applies, the function of evaluating internal financial controls and risk-management systems.[29] Although the provision does not expressly extend this function to AI governance or data protection, it illustrates the broader principle that significant organisational risks may require structured oversight within corporate governance mechanisms.

[28] Companies Act, No. 18 of 2013, § 166(3), India Code (2013)
[29] Id. § 177(4)(vii)

The applicability of these provisions must, however, be carefully distinguished according to the legal status and classification of the company. It would be incorrect to suggest that every private company is required under Section 177 to maintain an Audit Committee with responsibility for AI or data-protection risks. The provision applies to listed public companies and such other prescribed classes of companies. Accordingly, for private companies outside those categories, board oversight of data-protection risk may arise principally from the directors' broader governance responsibilities and the company's own internal governance arrangements rather than from a mandatory Audit Committee structure.

4.4 Significant Data Fiduciaries: A Stronger Governance Model

The DPDP Act provides its clearest statutory connection between data protection and organisational governance through the concept of the Significant Data Fiduciary. Section 10 permits the Central Government to notify a Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciaries after considering factors such as the volume and sensitivity of personal data processed and the risk posed to the rights of Data Principals, among other considerations.[30]

Once classified as a Significant Data Fiduciary, an entity is subject to additional obligations. Section 10(2) requires such an entity to appoint a Data Protection Officer who is based in India and is responsible to the Board of Directors or similar governing body. It also requires the appointment of an independent data auditor and the undertaking of periodic Data Protection.

Impact Assessments and audits.[31]

These requirements are particularly significant for the governance of AI-enabled data processing. They demonstrate that the DPDP framework recognises circumstances in which data protection requires organisational structures extending beyond ordinary operational compliance. The reference to responsibility to the Board of Directors or similar governing body is especially relevant because it establishes an express connection between data-protection functions and the highest level of corporate governance for Significant Data Fiduciaries.

At the same time, this provision establishes an important limit to the argument for universal

[30] Digital Personal Data Protection Act, No. 22 of 2023, § 10(1), India Code (2023)
[31] Id. § 10(2)

board oversight. The enhanced requirements under Section 10 are linked to the statutory classification of a Significant Data Fiduciary. They cannot automatically be extended to every private company merely because that company uses AI or processes personal data. The distinction strengthens rather than weakens the case for a proportionate governance approach: companies presenting greater risks may require stronger institutional oversight, while ordinary entities may adopt governance mechanisms appropriate to their scale and activities.

4.5 AI Deployment and the Limits of the DPDP Framework

AI introduces governance concerns that cannot all be resolved through data-protection law. An AI system may raise questions concerning discrimination, explainability, accuracy, intellectual property, employment consequences, competition and accountability even where the system does not process personal data in a manner falling within the DPDP Act. These issues demonstrate why the DPDP Act should not be presented as a comprehensive AI-governance statute.

The relevance of the DPDP framework to AI is instead strongest where the operation of an AI system involves the processing of digital personal data. In such circumstances, the company's obligations as a Data Fiduciary, including obligations relating to security safeguards and processing undertaken through Data Processors, become directly relevant. AI deployment therefore provides a significant context in which existing data-protection obligations may acquire new corporate-governance importance, but it does not transform those obligations into a general statutory code for governing AI.

This limitation is important for the development of responsible corporate governance. Companies should not assume that compliance with the DPDP Act alone makes an AI system legally or ethically acceptable. Conversely, boards should not be treated as legally responsible for every possible risk arising from AI merely because the company has adopted an AI system. A more defensible approach is to identify the specific legal risks created by the company's use of AI, determine whether personal-data processing is involved, and establish governance mechanisms proportionate to the significance of those risks.

4.6 From Compliance to Meaningful Board Oversight

The principal governance challenge is therefore to move beyond a narrow understanding of

compliance. A company may formally appoint responsible personnel, execute contracts with Data Processors and maintain security policies while still failing to ensure that its senior decision-makers understand the significance of data-related risks. Compliance becomes meaningful only when the organisation has mechanisms through which significant risks are communicated to the appropriate decision-makers and acted upon.

For private companies using AI to process personal data, board oversight should consequently focus on the governance of risk rather than the technical operation of AI systems. At a minimum, significant AI-related data risks should be capable of being identified, reported and escalated within the company's organisational structure. The board or governing body should receive sufficient information to determine whether the company's data-processing practices are consistent with its legal obligations and risk appetite.

Such an approach also recognises the respective roles of different actors. Technical teams are better placed to address cybersecurity architecture and system vulnerabilities; legal and compliance personnel can assess statutory obligations and contractual arrangements; management can coordinate implementation; and the board can exercise strategic oversight over material risks. Effective corporate governance lies not in transferring all these responsibilities to the board but in ensuring that they operate as part of a coherent accountability structure.

The DPDP framework thus provides an opportunity to reconsider the place of data protection within corporate governance. The growing use of AI makes that reconsideration particularly timely because the scale and complexity of data processing may increase as companies adopt automated systems. The appropriate response is neither to treat AI as a purely technical matter nor to impose unsupported statutory duties upon directors. It is to integrate significant dataprotection risks into existing corporate governance structures while maintaining a clear distinction between what the law requires and what constitutes good governance practice.

5. Important Case Laws and Policy Examples

5.1 *Justice K.S. Puttaswamy (Retd.) v. Union of India*

The decision of the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* provides the constitutional foundation for examining privacy and personal-data protection in

India. The nine-judge Bench unanimously recognised privacy as a constitutionally protected right arising from the guarantees of life and personal liberty under Article 21 and the freedoms guaranteed by Part III of the Constitution.[32] The Court's reasoning extended beyond physical privacy and recognised informational privacy as an important aspect of individual autonomy.

The judgment is significant to the present discussion because corporate use of data, including through technologically advanced systems, may directly affect an individual's ability to control information concerning them. Although the case did not deal with artificial intelligence or the DPDP Act, its recognition of informational privacy provides the constitutional background against which subsequent statutory regulation of personal data can be understood. For private companies deploying AI systems that process personal data, privacy therefore cannot be reduced to a purely contractual relationship between the company and the individual; it forms part of a broader legal framework protecting individual autonomy.

The significance of *Puttaswamy* should nevertheless be stated carefully. The judgment did not impose a general set of obligations upon private companies for AI deployment. Its importance lies principally in establishing privacy as a fundamental right and in identifying informational privacy as a constitutionally relevant interest. The specific duties of private companies arise through applicable statutory and regulatory frameworks.

5.2 *Karmanya Singh Sareen v. Union of India*

The Delhi High Court's decision in *Karmanya Singh Sareen v. Union of India* provides an earlier judicial illustration of concerns surrounding the collection and sharing of personal information by a private digital platform. The petitioners challenged aspects of WhatsApp's privacy policy, particularly the sharing of user information with Facebook and entities within the Facebook group.[33] The proceedings raised questions concerning privacy, user consent and the protection of personal information in the context of a widely used digital service.

The case is relevant to the present paper because it demonstrates that concerns surrounding private-sector data processing arose in Indian judicial discourse even before the enactment of the DPDP Act. It also illustrates the difficulty of addressing large-scale digital data practices through conventional contractual arrangements alone. The case predates the Supreme Court's

[32] J*ustice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[33] *Karmanya Singh Sareen v. Union of India*, W.P. (C) No. 7663 of 2016 (Delhi High Ct. Sept. 23, 2016).

nine-judge decision in *Puttaswamy* and the enactment of the DPDP Act; consequently, it should not be treated as establishing the present statutory standard for data protection. Its value lies instead in demonstrating the evolution of legal concerns surrounding private companies' control and use of personal information.[34]

For AI deployment, the underlying concern assumes a broader significance. AI systems can depend upon extensive datasets and may involve multiple stages of collection, storage and processing. Where such systems process personal data, questions concerning the purpose and scope of processing, the identity of entities involved and the security of information become increasingly important. The case therefore provides useful historical context for understanding why stronger statutory regulation of personal-data processing became necessary.

5.3 NITI Aayog's Responsible AI Framework

Judicial decisions alone do not provide the complete policy context for AI governance in India. NITI Aayog's *Approach Document for India: Part 1 – Principles for Responsible AI*, published in 2021, identified seven principles for responsible AI, including safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability, and protection and reinforcement of positive human values.[35]

The document is particularly relevant because it recognises privacy and security, transparency and accountability as important considerations in the design, development and deployment of AI. It also discusses the need for governance mechanisms that can address the risks associated with AI systems and recognises that the approach should evolve alongside technological developments.[36]

The framework is not legislation and therefore does not create enforceable statutory duties equivalent to those contained in the DPDP Act. Its significance for this paper is consequently normative rather than legislative. It demonstrates that responsible AI governance in India has already been discussed in terms of privacy, security and accountability, providing a useful policy context for considering how private companies may incorporate these concerns into their internal governance structures.

[34] Id.
[35] NITI Aayog, *Approach Document for India: Part 1—Principles for Responsible AI* (2021).
[36] Id.

NITI Aayog's subsequent *Approach Document for India: Part 2 – Operationalizing Principles for Responsible AI* further considered mechanisms for operationalising responsible-AI principles across different sectors, including the private sector. [37]The policy approach therefore supports the proposition that AI governance cannot depend exclusively upon technical development; organisational roles, accountability mechanisms and risk-based approaches also have a role to play.

5.4 Relevance of the Authorities to the Present Analysis

The authorities considered above reveal an important progression in the Indian legal and policy approach. *Karmanya Singh Sareen* illustrates early judicial concern regarding private-sector control and sharing of personal information. *Puttaswamy* subsequently established privacy, including informational privacy, as a constitutionally protected interest. The DPDP Act has since created a statutory framework governing digital personal-data processing, while NITI Aayog's responsible-AI framework demonstrates the policy recognition of privacy, security, transparency and accountability concerns arising from AI.

None of these authorities, taken individually, establishes a general rule that every private company's board is legally required to supervise AI systems. Nor do they establish a universal statutory obligation to conduct algorithmic audits. Their combined significance is instead in demonstrating why data protection and AI-related risks are increasingly relevant to corporate governance. The DPDP framework provides the binding statutory obligations; corporate law provides the broader governance structure; and responsible-AI policy provides guidance concerning the risks and principles that may inform corporate practice.

This distinction is central to the argument of the paper. A responsible governance model should be developed through the interaction of these legal and policy considerations without confusing a recommended governance practice with a mandatory statutory requirement. For private companies, the objective should therefore be to establish proportionate oversight mechanisms capable of identifying and responding to material data-protection risks associated with AI deployment.

[37] NITI Aayog, *Approach Document for India: Part 2—Operationalizing Principles for Responsible AI* (2021).

6. Findings and Suggestions

6.1 Findings

The analysis demonstrates that the DPDP framework has altered the legal significance of personal-data protection for private companies. Data protection can no longer be treated exclusively as an information-technology or compliance function where the processing of personal data forms an important part of the company's business operations. Section 8 of the DPDP Act places responsibility upon the Data Fiduciary for compliance even when processing is undertaken on its behalf by a Data Processor. The statutory framework therefore connects data protection with organisational responsibility rather than treating outsourcing as a complete transfer of accountability.[38]

A second finding is that the increasing use of AI strengthens the need to consider data protection within corporate risk management. AI systems frequently depend upon the collection, processing or analysis of data, and companies may rely upon external providers for part of that process. A vulnerability in the underlying data environment can consequently become a corporate risk extending beyond the technical functioning of the AI system itself. The significance of this risk is reinforced by the financial consequences associated with specified failures under the DPDP Act.[39]

At the same time, the legal framework does not support an argument that every private company deploying AI is subject to a mandatory regime of board-level AI governance. The DPDP Act does not expressly impose a general obligation upon directors to supervise AI systems, nor does it prescribe algorithmic audits for every AI deployment. Similarly, the Companies Act does not contain a provision specifically assigning responsibility for AI governance to directors. The stronger legal position is therefore to regard board oversight as arising from the broader governance and risk-management responsibilities applicable to the company, rather than as an independent universal statutory requirement created by the DPDP Act.

The position is different where an entity falls within the statutory category of a Significant Data Fiduciary. Section 10 expressly requires such entities to appoint a Data Protection Officer who

[38] Digital Personal Data Protection Act, No. 22 of 2023, § 8(1)–(2), India Code (2023).
[39] Id. § 33, sched

is responsible to the Board of Directors or similar governing body and to appoint an independent data auditor and undertake periodic Data Protection Impact Assessments and audits.[40] This demonstrates that the legislature has recognised circumstances in which the scale or nature of data processing justifies enhanced organisational accountability. It also indicates that a proportionate approach is more consistent with the structure of the Act than imposing identical governance requirements upon all private companies.

Another important finding concerns the relationship between corporate governance and technical expertise. Board oversight does not require directors to perform technical security assessments or evaluate the architecture of an AI model themselves. Such responsibilities are more appropriately allocated to qualified technical, legal and compliance personnel. The governance responsibility of the board lies in ensuring that appropriate structures exist, that material risks are brought to the attention of the appropriate decision-makers and that management has adequate mechanisms for responding to those risks. This division of responsibility prevents corporate governance from becoming either excessively technical or merely symbolic.

Finally, the analysis reveals a limitation in the present legal framework. The DPDP Act addresses the processing of digital personal data and associated obligations, but it does not constitute a comprehensive statute regulating the wider risks of artificial intelligence. Issues such as discriminatory outcomes, explainability, intellectual-property concerns and broader accountability questions may extend beyond the scope of data-protection law. Consequently, compliance with the DPDP framework should not be treated as equivalent to comprehensive AI governance.

6.2 Suggestions

Private companies using AI systems that process personal data should incorporate material data-protection risks into their existing enterprise risk-management structures. This does not necessarily require the creation of a separate board committee for AI in every company. Instead, companies should establish internal reporting mechanisms through which significant dataprotection risks, security incidents and material concerns arising from AI deployment can be escalated to senior management and, where appropriate, the board.

[40] Id. § 10(2).

Companies should also conduct appropriate due diligence before engaging external AI service providers or other Data Processors. Contracts with such entities should clearly identify the nature and purpose of processing, responsibilities concerning security, incident response and cooperation, and appropriate mechanisms for ensuring compliance with applicable dataprotection requirements. The statutory responsibility of the Data Fiduciary under Section 8(1) makes such arrangements particularly important because outsourcing does not eliminate the company's responsibility for processing undertaken on its behalf.[41]

A further recommendation is the establishment of an internal AI and data-governance policy proportionate to the company's activities. Such a policy may identify the categories of personal data processed by AI systems, the purposes of processing, the personnel responsible for oversight, procedures for addressing security incidents and criteria for escalating significant risks. For larger or higher-risk organisations, the policy may also provide for periodic assessments of AI-related data risks. Such measures should be understood as governance recommendations rather than as statutory requirements unless expressly mandated by applicable law.

Board-level oversight should also be proportionate to the nature and scale of the company's data-processing activities. Where AI systems process sensitive or substantial quantities of personal data, or where a significant reliance is placed upon external processors, the board should receive sufficient information to understand the associated legal and operational risks. For Significant Data Fiduciaries, the statutory requirement that the Data Protection Officer be responsible to the Board of Directors or similar governing body provides a more direct institutional mechanism for such oversight.[42]

Companies should further develop clear data-breach response procedures. A breach-response plan should identify the persons responsible for detecting, containing, investigating and reporting an incident and should establish a mechanism for timely escalation. This is particularly important because the DPDP framework contains obligations concerning notification of personal data breaches. Effective governance therefore requires preparation before an incident occurs rather than attempting to construct a response after a breach has already taken place.

[41] Id. § 8(1)–(2).
[42] Id. § 10(2)(a).

Finally, regulators and policymakers should continue to clarify the relationship between data protection and AI governance. As AI adoption increases, there may be situations in which existing data-protection obligations do not adequately address risks created by automated systems. Future regulatory development should therefore consider whether additional sectorspecific or risk-based governance mechanisms are necessary. Any such development, however, should distinguish between genuine regulatory gaps and matters that can appropriately be addressed through organisational policies, contractual controls and existing corporate governance mechanisms.

The objective should not be to create unnecessary layers of compliance. Instead, the regulatory approach should encourage companies to identify material risks at an early stage, assign responsibility clearly and maintain meaningful accountability for the processing of personal data through increasingly complex technological systems.

7. Conclusion

The growing use of artificial intelligence by private companies has made the relationship between data protection and corporate governance increasingly significant. AI systems that process personal data can create risks extending beyond technical security, particularly where companies depend upon external Data Processors or operate at a scale that makes a data breach capable of producing substantial legal, financial and reputational consequences. The Digital Personal Data Protection Act, 2023 ("DPDP Act") responds to these concerns by placing responsibility upon Data Fiduciaries for compliance and by requiring appropriate technical and organisational measures and reasonable security safeguards for preventing personal data breaches.[43]

The analysis demonstrates, however, that the DPDP Act should not be interpreted as a comprehensive statute governing artificial intelligence. Its principal statutory focus is the processing of digital personal data. AI therefore becomes relevant to the DPDP framework where its deployment involves processing of personal data within the scope of the Act. Wider questions concerning artificial intelligence that do not involve such processing cannot automatically be brought within the Act merely because an AI system is being used.[44]

[43] Digital Personal Data Protection Act, No. 22 of 2023, § 8(1), (4)–(5), India Code (2023)
[44] d. §§ 2–4.

The relationship between the DPDP framework and corporate governance is consequently one of interaction rather than substitution. The Companies Act, 2013 establishes broader duties of directors, including the obligation to exercise due and reasonable care, skill and diligence and to exercise independent judgment.[45]These duties provide an important corporate-governance context for considering significant organisational risks, but they should not be interpreted as creating an express, universal statutory duty upon every director to supervise AI systems or data-protection compliance.

The strongest statutory connection between data protection and board-level governance is found in the provisions concerning Significant Data Fiduciaries. Section 10 requires such entities to appoint a Data Protection Officer who is responsible to the Board of Directors or similar governing body and to appoint an independent data auditor and undertake periodic Data Protection Impact Assessments and audits.[46] This demonstrates that the legislature has recognised circumstances in which the nature and scale of data processing justify enhanced organisational oversight.

For other private companies, a proportionate governance approach is more appropriate. Boards should not be expected to perform the technical functions of cybersecurity teams or evaluate the detailed operation of every AI model. Their role should instead focus on ensuring that significant data-protection risks are identified, communicated and addressed through appropriate organisational structures. This approach is consistent with the distinction between operational responsibility and governance oversight and avoids attributing statutory duties to directors that the present legal framework does not expressly impose.

The issue is particularly important where processing is outsourced. Section 8(1) makes the Data Fiduciary responsible for compliance in respect of processing undertaken by it or on its behalf by a Data Processor, while Section 8(2) requires the engagement of a Data Processor for relevant activities to be under a valid contract.[47] Consequently, the use of external AI service providers does not by itself eliminate the Data Fiduciary's statutory responsibility. Companies must therefore treat the governance of third-party data-processing arrangements as part of their broader risk-management framework.

[45] Companies Act, No. 18 of 2013, § 166(3), India Code (2013)
[46] Digital Personal Data Protection Act, No. 22 of 2023, § 10(2), India Code (2023)
[47] Id. § 8(1)–(2).

Ultimately, responsible AI deployment requires companies to move beyond a narrow understanding of data-protection compliance. The DPDP framework provides the statutory foundation for protecting digital personal data, while corporate-governance principles provide mechanisms through which significant organisational risks may be identified and overseen. The increasing use of AI makes the interaction between these two areas more important, but it does not justify treating the DPDP Act as an all-encompassing AI-governance law.

The future development of Indian data and AI regulation should therefore seek to maintain an appropriate balance between technological innovation and accountability. Rather than imposing identical governance requirements upon every private company, the regulatory approach should remain proportionate to the scale, nature and potential impact of the risks involved. A governance model that clearly distinguishes statutory obligations from recommended corporate practices can encourage responsible AI deployment while ensuring that personal data entrusted to private companies is treated as a matter of legal and organisational responsibility.

Bibliography

A. Primary legal sources

Statutes

1. Companies Act, 2013, No. 18, Acts of Parliament, 2013 (India).

2. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

Rules And Regulations

3. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, pt. II, sec. 3(i) (Nov. 13, 2025).

Cases

4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

5. *Karmanya Singh Sareen v. Union of India*, W.P. (C) No. 7663 of 2016 (Delhi High Ct. Sept. 23, 2016).

B. Government and Policy Sources

6. NITI AAYOG, *Approach Document for India: Part 1—Principles for Responsible AI* (Feb. 2021).

7. NITI AAYOG, *Approach Document for India: Part 2—Operationalizing Principles for Responsible AI* (Aug. 2021).