INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

DATA DILIGENCE IN THE AGE OFAI: EVALUATING DATA PRIVACY AND AI ASSETS IN INDIAAND THE EUROPEAN UNION

AUTHORED BY - SUNAINA JAIN

CHAPTER 1: INTRODUCTION

1.1 Introduction

In recent decades, the nature of business enterprises has undergone a significant transformation due to rapid digitalisation. Modern companies increasingly rely on digital technologies, data-driven decision-making, and artificial intelligence systems to conduct their operations, expand markets, and generate value.[1] As a result, data and AI have emerged as critical components of contemporary business models across sectors such as finance, healthcare, e-commerce, and technology services.[2]

This transformation has directly affected the way companies are valued and acquired. In mergers and acquisitions, acquirers are no longer primarily interested in physical assets or traditional intellectual property alone. Instead, they focus on the quality of data held by the target company, the efficiency of its AI systems, and the scalability of its digital infrastructure.[3] These intangible assets often constitute the principal justification for high transaction valuations.[4]

Despite this shift, the legal frameworks governing corporate transactions have not evolved at the same pace. Traditional M&A due diligence practices continue to emphasise financial disclosures, contractual arrangements, and registered intellectual property, while treating data and AI systems as secondary or purely technical concerns.[5] This misalignment forms the starting point of the present research.

Traditional Due Diligence and Its Foundational Assumptions

Due diligence in mergers and acquisitions is traditionally understood as a risk-assessment

mechanism. Its primary purpose is to enable the acquiring entity to verify ownership of assets, identify liabilities, and assess compliance with applicable laws before completing a transaction.[6] Historically, this process developed in response to industrial and manufacturing-based business models, where assets were tangible, ownership was traceable, and risks were largely historical in nature.

Within this framework, legal due diligence focused on matters such as title verification, contractual enforceability, pending litigation, and statutory compliance. Intellectual property due diligence was confined to registered rights such as patents, trademarks, and copyrights. Information technology systems were examined largely from an operational or cybersecurity perspective, rather than as independent value-generating legal assets.

These assumptions were adequate when corporate value was primarily embedded in physical infrastructure or formal legal rights. However, they presupposed that assets were transferable objects and that compliance failures could be addressed through contractual protections such as representations, warranties, and indemnities. This assumption becomes problematic in the context of data-driven enterprises.

Emergence of Data and AI as Value-Defining Assets

The rise of the digital economy has altered the composition of corporate assets. Data, particularly personal data, and AI models trained on such data now function as the core drivers of innovation and competitive advantage.[7] Unlike traditional assets, data derives value from its volume, accuracy, diversity, and lawful usability. Artificial intelligence systems, in turn, rely on continuous data inputs and algorithmic learning processes to deliver commercial outcomes.

Crucially, data is not an asset whose value can be determined solely by possession or control. Its legal usability depends on compliance with data protection laws, validity of consent, purpose limitation, and security safeguards. Similarly, AI models are not discrete intellectual property objects but composite systems combining proprietary code, third- party components, licensed or scraped datasets, and probabilistic outputs.

This introduces a fundamental shift: the value of data and AI assets is conditional and reversible. An AI model may appear commercially valuable at the time of acquisition but can lose its legal legitimacy if the underlying data is found to be unlawfully collected or improperly processed. This conditionality distinguishes digital assets from traditional corporate property.

Regulatory Evolution and the Transformation of Legal Risk

The transformation of data into a regulated legal object has intensified with the enactment of modern data protection regimes. In India, the Digital Personal Data Protection Act, 2023 establishes an accountability-based framework that imposes statutory obligations on entities processing personal data.[8] In the European Union, the General Data Protection Regulation similarly emphasises lawful processing, data minimisation, and regulatory oversight.[9]

These regimes significantly alter the legal risk profile of corporate transactions. Liability under data protection law is not confined to future conduct but may extend to historical violations. In share acquisitions, acquiring entities inherit the compliance history of the target company and assume responsibility as data fiduciaries or controllers.[10] Regulatory authorities are empowered to impose substantial penalties irrespective of private contractual arrangements between parties.

As a result, data transitions from being a commercial asset to a potential source of regulatory exposure. Traditional due diligence mechanisms, which rely on contractual risk allocation and historical compliance review, are insufficient to capture this forward- looking and inheritable liability.

Algorithmic Accountability and Advanced Risk Considerations

Beyond data protection compliance, artificial intelligence systems introduce an additional layer of legal complexity in the form of algorithmic accountability. AI models increasingly influence decisions affecting individuals 'access to employment, credit, insurance, and public services. Consequently, concerns regarding algorithmic bias, discrimination, and transparency have attracted regulatory and legal scrutiny.[11]

Algorithmic risks are inherently structural and prospective. Bias may be embedded within training data or model architecture and may not manifest until the system is deployed at scale. Traditional due diligence processes, which focus on past litigation and existing regulatory action, are ill-equipped to detect such latent risks. The acquirer therefore inherits not only past compliance failures but also the potential for future legal violations arising from the design of the AI system itself.

This marks a departure from conventional notions of corporate risk, where liability is primarily backward-looking. In the AI context, liability is closely linked to the operational characteristics of the acquired asset.

From Basic Compliance to Advanced Due Diligence

The foregoing analysis demonstrates a gradual but decisive shift in the nature of corporate assets and associated legal risks. At a basic level, data and AI appear as technological tools supporting business efficiency. At an intermediate level, they emerge as core drivers of enterprise value. At an advanced level, they function as legally regulated processes whose continued use depends on sustained compliance with evolving regulatory standards.

This progression necessitates a corresponding evolution in due diligence methodology. Due diligence must move beyond checklist-based compliance reviews and adopt a structured approach capable of examining data provenance, regulatory accountability, algorithmic integrity, and AI asset sustainability. This conceptual shift underpins the rationale for developing a Data and AI Due Diligence framework, as articulated in the present research.

1.2 Statement of The Problem

In mergers and acquisitions, due diligence functions as a legal mechanism for allocating risk between the buyer and the seller. Traditionally, it focuses on verifying asset ownership, statutory compliance, and existing liabilities, with the assumption that identified risks can be managed through contractual tools such as representations, warranties, and indemnities. This approach was developed for conventional businesses where assets and liabilities were finite and historically traceable.

However, this framework is inadequate for data-driven and AI-enabled enterprises. Modern data protection laws impose continuous, accountability-based obligations on companies that process personal data. In share acquisition transactions, acquiring entities inherit responsibility for the target company‘s past data processing practices, even where violations occurred prior to the acquisition. Regulatory authorities may impose penalties irrespective of private contractual arrangements, rendering traditional risk-allocation mechanisms insufficient.

The problem is further compounded by the legal nature of data and artificial intelligence. Data is not a freely transferable asset; its lawful use depends on ongoing compliance with regulatory requirements such as valid consent and purpose limitation. Artificial intelligence systems are composite assets dependent on training data, third-party software, and algorithmic processes,

where legal defects particularly in training data may irreversibly destroy commercial value.

Consequently, traditional due diligence frameworks, which are ownership- and contract- centric, fail to identify and manage inherited regulatory and algorithmic risks. This inability to assess the legal sustainability of data and AI assets constitutes the central problem addressed by this dissertation.

1.3 Research Questions

1. How has the transformation of data and artificial intelligence into core corporateassets altered the legal foundations of due diligence in mergers and acquisitions?
2. Why are traditional M&A due diligence frameworks inadequate for identifying regulatory and compliance risks associated with data-driven and AI-enabled enterprises?
3. How does inherited liability under modern data protection laws affect risk allocation and valuation in share acquisition transactions?
4. In what ways does the legal character of data as a regulated process, rather than a transferable asset, disrupt property-centric and IP-centric corporate law doctrines?
5. Why do artificial intelligence systems expose fundamental limitations in traditional intellectual property–focused due diligence, particularly in relation to training data provenance and AI-generated outputs?
6. Can a structured Data and AI Due Diligence framework realign M&A practice with contemporary data protection and AI governance regimes in India and the European Union?

1.4 Research Objectives

1. To examine the transformation of data and artificial intelligence into core corporate assets and its implications for traditional due diligence frameworks in mergers and acquisitions.
2. To critically analyse the structural inadequacies of existing M&A due diligence mechanisms in identifying regulatory, compliance, and algorithmic risks associated with data-intensive enterprises.
3. To evaluate the impact of inherited liability under contemporary data protection laws on risk allocation, valuation, and contractual safeguards in share acquisition transactions.

4. To analyse the legal character of data as a regulated legal process rather than a transferable asset, and its consequences for property-centric and IP-centric corporate doctrines.
5. To examine the limitations of intellectual property–focused due diligence in addressing legal risks associated with artificial intelligence systems, particularly in relation to training data provenance and AI-generated outputs.
6. To develop and evaluate a structured Data and AI Due Diligence framework capable of mitigating inherited regulatory liability and valuation distortion in M&A transactions within India and the European Union.

1.5 Hypothesis

1. Traditional M&A due diligence frameworks are structurally inadequate to assess the legal risks associated with data-driven and AI-enabled enterprises because they are grounded in ownership-centric and retrospective models of risk allocation that fail to capture continuous regulatory compliance obligations under modern data protection and AI governance regimes.
2. Inherited liability under contemporary data protection laws fundamentally undermines the effectiveness of contractual risk-allocation tools such as representations, warranties, and indemnities in share acquisition transactions.
3. Artificial intelligence systems disrupt traditional IP-centric corporate doctrines by introducing composite assets whose legal validity depends on data provenance, regulatory compliance, and algorithmic accountability rather than on formal ownership or registration alone.

1.6 Review of Literature

1. Avtar Singh (2020) analysed the foundational principles of company law in India in his work *"Company Law"*[12] and discussed the role of due diligence as a mechanism for identifying liabilities and allocating risk in corporate transactions, particularly mergers and acquisitions. He emphasised that traditional due diligence is structured around ownership verification and statutory compliance.
2. L. C. B. Gower and Paul Davies (2016) examined mergers, acquisitions, and corporate restructuring in *"Principles of Modern Company Law"*[13] and argued that due diligence,

representations, and warranties function as core tools for managing transactional risk, though their analysis remains focused on conventional asset-based enterprises.

3. Ramaiya (2019) analysed corporate restructuring and amalgamations under Indian company law in *"Guide to the Companies Act"*[14] and discussed the legal framework governing mergers, schemes of arrangement, and shareholder protection, while treating due diligence primarily as a procedural safeguard rather than a regulatory risk assessment tool.
4. Umakanth Varottil (2018) examined mergers and acquisitions in India in his scholarly writings on Indian corporate law and argued that Indian M&A practice is heavily contract-centric, relying on representations, warranties, and indemnities, with limited engagement with public law and regulatory risk.[15]
5. Umakanth Varottil (2014) analysed corporate governance and risk allocation in Indian companies in his work on corporate regulation and concluded that Indian corporate law places greater emphasis on private ordering, often overlooking continuous regulatory compliance obligations.[16]
6. Somasekhar Sundaresan (2017) examined securities regulation, corporate transactions, and regulatory enforcement in India in his writings on corporate and securities law and highlighted the growing interaction between regulatory compliance and corporate structuring in mergers and acquisitions.[17]
7. Gower, Davies, and Worthington (2018) analysed corporate restructuring and risk allocation mechanisms in mergers and acquisitions and discussed how due diligence traditionally operates within a private law framework, assuming that liabilities are finite and contractually manageable.[18]
8. Daniel J. Solove (2001) analysed privacy as a system of legal governance in *"Privacy as Legal Governance"*[19] and argued that modern regulatory regimes impose accountability-based obligations on organisations, which has significant implications for corporate liability.
9. Julie E. Cohen (2019) examined informational capitalism in *"Between Truth and Power"*[20] and argued that data has become a central corporate asset shaping market power and enterprise valuation.
10. Shoshana Zuboff (2019) analysed data-driven business models in *"The Age of Surveillance*

Capitalism"[21] and concluded that large-scale data extraction has transformed corporate strategy and raised new regulatory risks.

11. Christopher Kuner (2017) analysed GDPR enforcement and regulatory continuity in his work on EU data protection law and argued that liability under data protection regimes attaches to corporate entities irrespective of changes in ownership.[22]
12. The Organisation for Economic Co-operation and Development (2013) examined privacy governance in the *OECD Privacy Framework* and emphasised accountability-based compliance, which influences corporate governance and transactional risk.[23]

1.7 Research Gap

The review of existing literature reveals a clear and multi-layered research gap.

First, while data protection scholarship extensively analyses accountability, consent, and regulatory enforcement, it does not address how these obligations operate within mergers and acquisitions. In particular, the concept of **inherited regulatory liability**where acquirers assume responsibility for historical data processing violations remains under- theorised in corporate law discourse.

Second, AI governance literature focuses primarily on ethical deployment, bias, and public law regulation. These works conceptualise AI risk as a matter of societal harm and regulatory oversight, but fail to examine AI systems as **commercially acquired assets** whose legal defects can collapse transaction value.

Third, traditional M&A and corporate law literature continues to treat due diligence as an ownership- and contract-centric exercise. It assumes that risk can be adequately allocated through representations, warranties, and indemnities. This assumption is incompatible with data protection and AI governance regimes, where liability arises from continuous regulatory obligations beyond private contractual control.

Fourth, intellectual property scholarship identifies uncertainty surrounding AI training data and AI-generated outputs but does not situate these uncertainties within transactional contexts. The implications of AI IP ambiguity for valuation, enforceability, and post- acquisition viability are

largely unexplored.

Consequently, there exists no integrated doctrinal framework that connects data protection law, AI governance, and M&A due diligence.There is a specific absence of comparative legal scholarship examining how privacy regulation and algorithmic accountability reshape risk allocation, valuation, and due diligence practices in jurisdictions such as India and the European Union.

This dissertation addresses this gap by developing a Data and AI Due Diligence framework that reconceptualises due diligence as a process of regulatory sustainability assessment, rather than mere ownership verification, thereby aligning corporate transactional practice with contemporary data protection and AI governance regimes.

1.8 Research Methodology

This study employs a **doctrinal legal research methodology**, supported by **comparative legal analysis**, to examine the legal treatment of data and artificial intelligence in corporate transactions. The research is analytical in nature and focuses on the interpretation of statutes, regulatory frameworks, judicial decisions, and scholarly literature relevant to data protection, AI governance, and mergers and acquisitions. No empirical surveys, interviews, or quantitative techniques are used, as the research addresses doctrinal and regulatory questions rather than behavioural or technical issues.

Doctrinal analysis is used to evaluate the legal foundations of due diligence in mergers and acquisitions and to assess how accountability-based data protection regimes alter traditional assumptions of risk allocation in corporate law. The study examines the legal character of data as a regulated process and analyses the extent to which intellectual property–centric doctrines fail to accommodate the composite and compliance-dependent nature of AI systems. This approach enables identification of structural gaps between conventional corporate law practices and contemporary regulatory obligations, particularly in relation to inherited liability and regulatory continuity.

A comparative legal approach is adopted to analyse and contrast the regulatory frameworks

governing data and AI assets in India and the European Union. The Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation are examined to understand differences in regulatory design, enforcement mechanisms, and their impact on corporate due diligence and post-acquisition liability. Comparative analysis is used to draw normative insights relevant to business law and transactional practice.

The research is based exclusively on secondary legal sources, including statutes, regulatory guidelines, judicial decisions, academic commentaries, and reports issued by recognised international bodies. These materials are analysed thematically to examine issues of regulatory accountability, corporate compliance, and the legal sustainability of data and AI assets in mergers and acquisitions.

The study excludes technical evaluation of algorithms, economic valuation models, and empirical assessment of business practices, as such inquiries fall outside its doctrinal scope. Although the research is limited to the legal frameworks of India and the European Union and depends on existing regulatory material that may evolve, these limitations do not affect the validity of the doctrinal analysis undertaken.

1.9 Chapter Scheme

- Chapter I: Introduction: Data, Artificial Intelligence, and Corporate Transactions

This chapter introduces the research problem within the framework of Business Law. It examines how data and artificial intelligence have emerged as core corporate assets influencing enterprise valuation, mergers, and acquisitions. The chapter explains the inadequacy of traditional corporate due diligence in addressing data privacy and AI- related risks and situates the study within the domain of corporate transactions and risk allocation. It sets out the statement of the problem, research questions, objectives, hypotheses, scope, and methodology, with specific emphasis on mergers and acquisitions and corporate compliance.

- Chapter II: Historical Evolution of Data and AI as Corporate Assets and Due Diligence in Business Law

This chapter traces the historical evolution of data and artificial intelligence as corporate and

commercial assets rather than purely technological tools. It examines the development of due diligence as a risk-allocation mechanism in corporate transactions and explains how traditional M&A practices evolved in an industrial-era business environment. The chapter further analyses how data gradually transitioned from an operational resource to a value-defining corporate asset and why corporate law failed to adapt its due diligence frameworks to this shift.

- Chapter III: Corporate and Legislative Framework Governing Data Protection and AI Assets

This chapter analyses the statutory framework governing data and AI assets from a corporate law perspective. It examines the Digital Personal Data Protection Act, 2023, relevant provisions of the Information Technology Act, 2000, and allied corporate compliance obligations affecting business entities. The chapter focuses on the impact of these statutes on corporate governance, data fiduciary obligations, enterprise liability, and transaction structuring in mergers and acquisitions. It evaluates how statutory compliance affects valuation, ownership, and transfer of data and AI assets in corporate transactions.

- Chapter IV: Judicial Approach to Data Privacy, Corporate Liability, and Technology-Driven Businesses

This chapter examines judicial decisions that influence corporate liability and business risk in the context of data protection and technology-driven enterprises. It analyses how courts have interpreted privacy, organisational accountability, and compliance duties of corporations. The chapter focuses on judicial reasoning that affects corporate governance, regulatory exposure, and transactional risk in mergers and acquisitions involving data- intensive businesses, rather than on abstract constitutional doctrine.

- Chapter V: Comparative Analysis of Data Protection under the Indian DPDP Act, 2023 and the EU GDPR

This chapter undertakes a comparative corporate law analysis of the Indian DPDP Act, 2023 and the EU GDPR. It examines how both regimes regulate corporate data processing, impose fiduciary and compliance obligations on business entities, and create inherited liability in share acquisitions.

The chapter evaluates the implications of these regimes for corporate due diligence, valuation, and post-acquisition compliance risk, drawing lessons for Indian business law from EU corporate practice.

- Chapter VI:Conclusion and Suggestions

The final chapter consolidates the findings of the study from a business law perspective. It evaluates the research hypotheses and summarises how traditional corporate due diligence frameworks are inadequate for data-driven and AI-enabled enterprises. The chapter proposes corporate law–oriented suggestions, including the adoption of structured Data and AI Due Diligence mechanisms, enhanced board-level compliance oversight, and improved contractual risk-allocation strategies in mergers and acquisitions. It also identifies future directions for reform in business law and corporate regulation.

1.10 Student Learning Outcomes

Upon completion of this dissertation, the student will gain a clear and advanced understanding of data and artificial intelligence as core corporate assets influencing mergers and acquisitions and enterprise valuation. The student will be able to critically analyse the doctrinal foundations of due diligence in corporate law and evaluate its effectiveness as a mechanism of legal risk allocation in data-driven transactions. The study will equip the student with the ability to assess corporate compliance obligations under modern data protection and AI governance regimes, including the implications of inherited regulatory liability in share acquisitions. The student will further develop competence in applying statutory and judicial analysis to business law problems, conducting comparative analysis between the Indian DPDP Act, 2023 and the EU GDPR, and identifying best practices for corporate governance and due diligence. Finally, the dissertation will enhance doctrinal research and legal writing skills, enabling the student to provide informed legal analysis and professional advice in relation to data- and AI- intensive business transactions.

CHAPTER-II

HISTORICAL EVOLUTION OF DATA AND AI AS CORPORATE ASSETS AND DUE DILIGENCE IN BUSINESS LAW

2.1. Overview

This chapter explores the history behind three legal areas: M&A law and due diligence, data privacy, and the rise of data and AI as commercial assets. It argues that today‘s "data diligence" isn't a new invention. Instead, it‘s the result of forty years of slow shifts in corporate, privacy, and intellectual property law.

Early M&A diligence focused on physical assets and clear liabilities. In that era, ownership was easy to prove and risks were easier to contain. Back then, privacy rules mostly covered state secrets or specific professional duties; data wasn't seen as a valuable asset on its own.

Everything changed in the 1980s. Digitization and global markets pushed companies to find value in intangibles like software, databases, and algorithms. Europe began building data laws based on human rights and autonomy, while India‘s privacy norms took a slower path through constitutional law. M&A experts soon realized that a company‘s true worth often lived in its information, not its inventory.

Mapping this history is vital for today‘s deals. Modern risks like inherited legal liabilities or "toxic" datasets stem from laws originally written for a different world. We now see data diligence sitting right where corporate risk meets government accountability.

2.2. Historical Timeline

Year	India Development	EU Development	Relevance to Data/AI Diligence
1984	Companies Act 1956 dominant framework	Council of Europe Convention 108 (1981, in force)[24]	Early privacy norms separate from M&A
1991	Economic liberalization	Single Market deepening	Cross-border deals increase

1995	—	EU Data Protection Directive[25]	First comprehensive EU data regime
2000	IT Act 2000 enacted[26]	E-commerce Directive	Legal recognition of electronic data
2002	Competition Act 2002[27]	EU Merger Regulation reform	Formal merger control regimes
2008 – 11	SPDI Rules under IT Act[28]	Article 29 WP guidance	Corporate data compliance begins
2017	Puttaswamy judgment[29]	GDPR adopted (2016, applied 2018)[30]	Privacy as right; heavy penalties
2023	DPDP Act 2023[31]	AI Act (political agreement 2023–24)	Data/AI enter compliance-focused diligence

2.3. M&A Law Evolution

India‘s M&A laws find their roots in the Companies Act, 1956.[32] This framework focused on formal legal processes like amalgamations and reconstructions, which usually required a court's stamp of approval. At the time, the law assumed a company's value came from physical assets, contracts, and clear debts. Under sections 391–394 of the Act, judges focused on making sure shareholders and creditors were treated fairly. They didn't really dig into the deep commercial risks of the deals themselves.

During these early years, "due diligence" wasn't a formal legal requirement. Instead, it was a routine practice for lawyers and accountants. They checked property titles, tax bills, and ongoing lawsuits. The underlying belief was that assets were physical things you could touch and transfer, and risks were mostly issues from the past. If a company owned data, it was treated as a minor detail rather than a core part of the business's value.

The 1991 economic reforms changed everything.[33] Liberalization opened India to foreign investment and sparked rapid private growth. As Indian companies started playing on the global stage, deals became more complex. Foreign buyers brought more intense auditing styles with

them. Even so, diligence still mostly focused on taxes and basic corporate rules. Information assets remained largely ignored.

A major shift happened with the Competition Act, 2002.[34] This law introduced mandatory "merger control," bringing public oversight to what used to be private deals. The Competition Commission of India (CCI) began checking if big mergers would hurt the market. This forced companies to include regulatory risks in their deal-making and expanded the scope of legal audits.

Despite this progress, the foundation of due diligence stayed stuck in the old way of verifying physical property. Even as India's tech sector exploded, the law didn't immediately adapt to check for things like data security or AI risks. Historically, Indian M&A law was built to protect investors and manage market power not to audit the legal health of data-driven business models. This history explains why data-focused diligence has been slow to arrive.

2.4. Historical Trajectory of Data Protection in India

The evolution of Indian data protection jurisprudence reveals a transition from fragmented, sectoral regulations to a unified, rights-based framework. Historically, India lacked a consolidated statutory regime dedicated to data privacy. Legal obligations regarding confidentiality were largely derived from the Indian Contract Act, 1872, fiduciary principles, and specific regulations governing the banking, telecommunications, and healthcare industries. During this era, the legal system perceived privacy primarily through the lens of physical protections such as safeguards against unauthorized search and seizure or telephone tapping rather than as a distinct, intangible right to informational autonomy.

The inaugural legislative attempt to address the digital landscape was the Information Technology Act, 2000.[35] While groundbreaking, its primary objective was the facilitation of electronic commerce through the legal recognition of digital signatures and electronic records. Although the Act introduced penalties for unauthorized access and cybercrimes, it lacked a comprehensive architecture for data protection. Its framework remained transactional and security-oriented, prioritizing the integrity of electronic communication over the individual's right to privacy.

A significant shift toward corporate accountability occurred with the notification of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.[36] These rules mandated that "body corporates" handling sensitive personal information implement privacy policies, obtain explicit consent, and maintain "reasonable" security standards. While this represented a move toward compliance-based regulation, enforcement mechanisms remained nascent. Consequently, during this period, data protection was rarely viewed as a critical risk factor in corporate mergers and acquisitions (M&A).

The most profound doctrinal shift was precipitated by the Supreme Court of India's landmark ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[37] The Court unanimously declared the right to privacy a fundamental right under the Constitution of India, characterizing it as an essential component of human dignity and liberty. By recognizing the principle of "informational self-determination," the judiciary elevated data protection from a peripheral commercial concern to a core constitutional mandate.

Despite this constitutional milestone, the integration of these principles into corporate practice was not immediate. For several years, data-related risks remained a secondary consideration in due diligence processes, typically confined to targets in highly regulated sectors. It was only through the increasing influence of global regulatory standards most notably the European Union's General Data Protection Regulation (GDPR) that Indian corporate actors began to internalize the potential liabilities associated with data processing. Thus, the historical narrative of Indian data law is defined by a gradual metamorphosis from sectoral confidentiality to a comprehensive, rights-centric compliance model. This historical lag explains the late maturation of data-centric diligence in the Indian M&A market.

2.5. Emergence of AI and Data as Commercial Assets

The transformation of data and Artificial Intelligence (AI) into central commercial assets occurred through industry practice rather than sudden legislative innovation. During the late 1990s, the growth of the IT and Business Process Outsourcing sectors began to redefine enterprise value, where valuation was increasingly driven by intangible resources like proprietary software and customer databases.[38]

Despite this commercial reality, the Indian legal system lacked a dedicated regime for data property. Instead, these assets were adapted into existing frameworks, such as the Indian Copyright Act, 1957. While copyright law acknowledges computer programs as "literary works," the status of raw or aggregated datasets remains precarious.[39] Unlike the European Union's *sui generis* database rights, Indian law has not recognized datasets as a distinct category of property, leaving them to be protected indirectly through trade secret principles and breach of confidence actions.[40]

AI systems initially entered the market as extensions of software services, valued for functional output rather than as independent legal assets. Historically, technology acquisition agreements focused on conventional metrics: licensing terms and standard Intellectual Property (IP) ownership. Issues now considered critical, such as the lawful provenance of training datasets or algorithmic bias, were largely absent from earlier legal discourse.

This historical narrative reflects a conspicuous rift between commercial practice and legal doctrine. While business valuations transitioned toward data-driven models, the law continued to treat data as incidental to traditional IP. This doctrinal lag explains why modern challenges such as ensuring lawful data provenance emerged in a legal environment not originally designed for data-intensive enterprises.

2.6. Evolution of European Union Merger and Acquisition Jurisprudence

The historical progression of Mergers and Acquisitions (M&A) law within the European Union is inextricably linked to the overarching objective of European market integration. Diverging from purely domestic corporate legal frameworks, EU merger control was forged within the crucible of competition law to prevent distortions within the internal market. This legal philosophy rests upon the premise that corporate concentrations possess the capacity to restructure market dynamics, thereby influencing cross-border trade and consumer welfare.[41]

Before the implementation of a centralized oversight mechanism, merger control was characterized by a fragmented landscape of national regulations. Large-scale, cross- border transactions were frequently subjected to redundant reviews by multiple Member States, a process

that engendered significant regulatory friction and economic inefficiency. The introduction of Council Regulation (EEC) No. 4064/89 signaled a pivotal transition toward supranational governance.[42] By establishing the "Community dimension" threshold, the Regulation granted the European Commission exclusive jurisdiction over significant concentrations, effectively streamlining the approval process for major entities.

This shift was structurally transformative, as it embedded public-law scrutiny into the heart of transnational corporate restructuring. Consequently, transactions ceased to be governed exclusively by private contracts or internal company law; instead, they became subject to rigorous competition-based assessments focused on market dominance and adverse competitive effects. The imposition of mandatory prior notifications and standstill obligations ensured that regulatory clearance became a condition precedent to the consummation of any major deal.

Such a robust regulatory architecture fundamentally altered the scope of European due diligence. Starting in the 1990s, the necessity of obtaining competition clearance transitioned from a secondary concern to a primary transactional risk. Legal practitioners expanded diligence protocols to incorporate sophisticated market share analyses, competitor mapping, and the evaluation of potential structural or behavioral remedies.[43] This historical integration of merger control into the planning phase of a transaction fostered a corporate culture where regulatory compliance was viewed as inseparable from deal structuring.

Subsequent legislative refinements, most notably Council Regulation (EC) No. 139/2004, modernized the substantive legal standard by moving from a "dominance" test to the "significant impediment to effective competition" (SIEC) criterion.[44] This evolution allowed the Commission to adopt a more nuanced analytical framework, further institutionalizing economic assessment within the review process. Historically, EU M&A law flourished in an environment where public-law considerations were central to the transaction. However, early iterations of this regime did not prioritize informational assets. Market power was traditionally quantified through production capacities and distribution networks rather than digital capital. It was only with the advent of the digital economy that data concentration began to permeate competition analysis, demonstrating a doctrinal evolution that addressed structural market risks long before adapting to data- driven

commercial models.

2.7. The Conceptual Lineage of European Data Protection

The historical trajectory of the European Union‘s data protection framework is fundamentally distinguished by its grounding in a robust human rights discourse. Early iterations of privacy protection in Europe were heavily influenced by post-war legal instruments, most notably Article 8 of the European Convention on Human Rights, which safeguards the sanctity of private and family life.[45] These foundational norms established a legal culture where data protection was not merely a commercial regulation but a critical extension of individual autonomy and human dignity.

The first binding international instrument to address these concerns was the Council of Europe‘s Convention 108, adopted in 1981.[46] This convention recognized the burgeoning risks associated with the automated processing of personal information, reflecting a precocious awareness of the implications of computerization. Historically, Convention 108 codified the seminal principles of fair processing, purpose limitation, and data quality tenets that would eventually serve as the bedrock for subsequent Union legislation.

A significant legislative milestone was reached with the enactment of the Data Protection Directive 95/46/EC, which inaugurated the first comprehensive transnational data regime within the EU.[47] This Directive sought to reconcile two potentially competing interests: the protection of fundamental rights and the unhindered flow of personal data across the internal market. The historical significance of this "balancing function" cannot be overstated, as it framed data protection as both a humanitarian necessity and a prerequisite for a functioning digital economy. Furthermore, by requiring Member States to establish independent supervisory authorities, the Directive institutionalized regulatory oversight across the continent.

During this era, corporate compliance cultures began to slowly internalize these mandates. Entities engaged in data processing were tasked with notifying national authorities and justifying their processing activities through specific legal bases. However, the intensity of enforcement remained inconsistent across various Member States, and compliance was frequently relegated to a matter

of administrative routine rather than being treated as a central strategic priority.

The transition from a fragmented directive model to a unified regulatory framework was completed with the application of the General Data Protection Regulation (GDPR) in 2018.[48] By utilizing the legal form of a regulation, the EU ensured direct applicability and uniformity across all Member States. The introduction of severe administrative penalties reaching up to 4% of an undertaking's global annual turnover historically transformed data protection from a technical footnote into a primary concern for corporate governance. The mandates for data protection officers, mandatory impact assessments, and the overarching principle of accountability embedded compliance directly into the structural fabric of corporate entities.

Crucially, the GDPR codified the principle that data protection obligations are inherently attached to the processing entity rather than to isolated acts. This ensures a continuity of responsibility that persists even through corporate reorganizations or acquisitions. Historically, this doctrinal shift was instrumental in the emergence of specialized data- related due diligence in M&A transactions involving European entities. Consequently, the EU‘s regulatory evolution reflects a rights-driven path that has successfully intersected with modern corporate governance, fostering a culture where data integrity is viewed as both a legal obligation and an ethical imperative.

2.8. The Commercial Recognition of Data and AI Assets in the European Union

The conceptualization of data and artificial intelligence as commercially significant assets within the European Union matured through the specialized lenses of intellectual property and information law, rather than through traditional corporate law doctrines. A pivotal moment in this trajectory was the enactment of the Database Directive 96/9/EC.[49] This instrument introduced a *sui generis* right, specifically designed to protect databases where a "substantial investment" had been made in the acquisition, verification, or presentation of their contents. Historically, this represented a profound legal innovation; it moved beyond the requirement of creative authorship to recognize the economic value inherent in the diligent collection of data itself.

The establishment of this *sui generis* right served as an early acknowledgment of the burgeoning economic power of data aggregation. By providing a legal safeguard for investment, the Directive

incentivized data-intensive industries and fundamentally altered the treatment of datasets in commercial negotiations. However, the framework maintained a delicate equilibrium: it protected the investment and structure of the database without granting proprietary control over the underlying facts, thereby preserving a necessary degree of informational freedom.

Parallel to these developments, the economic significance of computer programs was codified under the Software Directive, which categorized software as a "literary work" for copyright purposes.[50] This facilitated a robust licensing culture that became the cornerstone of European technology transactions. Furthermore, the protection of proprietary algorithms and confidential business methods was eventually harmonized through the Trade Secrets Directive, providing a more predictable legal environment for the safeguarding of "black-box" technologies.[51]

In historical practice, AI systems emerged within the European market primarily through the financial, telecommunications, and digital service sectors. In these early stages, algorithmic tools were largely viewed as auxiliary components of broader software or service packages rather than as autonomous legal assets. Consequently, their commercial valuation was dictated by functional performance and contractual stipulations rather than by a distinct legal identity.

Nevertheless, the strategic importance of data eventually gained the attention of European competition authorities. Regulatory investigations increasingly began to treat access to expansive datasets as a critical parameter for evaluating market power.[52] This marked a significant shift toward recognizing data as a structural resource capable of influencing competitive dynamics.

While the European Union moved more rapidly than jurisdictions like India to institute dedicated legal instruments for information-intensive assets, a certain doctrinal lag remained evident. Even within the EU, AI systems continued to be categorized under existing intellectual property and trade secret frameworks rather than being recognized as an entirely new class of assets. This historical layering of various legal regimes explains why contemporary data-driven due diligence requires a sophisticated navigation of multiple, overlapping doctrines rather than reliance on a unified legal theory.

2.9. Rights Orientation versus Market Orientation

The EU's data protection regime has historically been grounded in fundamental rights discourse. This tradition is visible in Article 8 of the European Convention on Human Rights, which recognizes the right to respect for private and family life.[53] The Council of Europe's Convention 108 further embedded privacy protection into a transnational legal framework focused on automated data processing.[54]

This rights-based orientation meant that data protection was not merely an instrument of market regulation but an expression of personal autonomy and dignity. Corporate obligations regarding data were thus framed as duties owed to individuals rather than as mere compliance requirements. Scholars have noted that European data protection law developed as a constitutional project as much as a regulatory one.[55]

India's historical trajectory differed. For decades, data governance was not framed as a matter of fundamental rights but as a matter of commercial reliability and cyber security. The Information Technology Act, 2000 primarily aimed to facilitate electronic commerce and recognize digital signatures.[56] Its orientation was transactional and security-focused, not rights-based. Corporate obligations arose from contract, tort, and sectoral norms rather than from a unified privacy doctrine.

Only with Justice K.S. Puttaswamy v. Union of India did privacy gain explicit constitutional recognition.[57] This judicial articulation marked a doctrinal shift, but historically it arrived after decades of market-driven digital expansion. Thus, the Indian model reflects a trajectory where economic modernization preceded rights-based data regulation.

This divergence affected corporate conduct. European firms historically encountered data protection as a structural obligation integrated into governance, whereas Indian firms often treated it as a developing regulatory requirement. As a result, the EU developed a stronger early culture of data-related compliance within corporate risk management.

2.10. Regulatory Timing and Institutional Maturity

Timing operates as a structural variable in legal development because regulatory intervention not only constrains behaviour but also shapes institutional expectations and market norms. In the field of data governance, the European Union's earlier adoption of comprehensive regulatory frameworks created a long-term path dependency that influenced corporate conduct, professional specialization, and transactional practice.

The adoption of Directive 95/46/EC in 1995 represented a watershed moment in transnational data regulation.[58] By mandating independent supervisory authorities, data processing principles, and cross-border safeguards, the Directive created an institutional ecosystem around data protection. Even where enforcement intensity differed among Member States, the mere existence of dedicated regulators normalized the idea that personal data processing was a matter of legal oversight rather than private discretion. Over time, this regulatory architecture encouraged the development of professional roles privacy officers, compliance auditors, and data governance consultants whose expertise became embedded in corporate operations.

Historically, this early institutionalization had cascading effects. Once firms invested in compliance infrastructures, internal reporting mechanisms, and governance protocols, data protection ceased to be an episodic concern and became a continuous compliance function. This institutional maturity later translated into transactional contexts: acquirers began to request evidence of compliance programs, audit trails, and regulatory correspondence during due diligence.

India's trajectory differed in both timing and structure. For many years, data regulation remained fragmented across sectoral and contractual norms. The Information Technology Act, 2000 recognized electronic records and cyber offences but did not create a full- fledged data protection regime.[59] The SPDI Rules of 2011 introduced obligations relating to consent and security practices, yet they lacked the institutional architecture of independent supervisory authorities with broad investigative powers.[60]

As a result, the visibility of enforcement remained limited. Compliance incentives were therefore

weaker, and corporate investment in privacy governance developed unevenly. Historically, this meant that Indian corporations often approached data governance pragmatically, calibrating compliance efforts to sectoral risk rather than to a uniform regulatory expectation. The absence of a mature enforcement ecosystem delayed the integration of data governance into routine corporate due diligence.

Thus, regulatory timing influenced not only doctrinal development but also corporate culture. Earlier intervention in the EU created structural expectations of compliance; later intervention in India produced a more gradual adaptation.

2.11. Judicial versus Legislative Leadership

The relative roles of courts and legislatures in shaping data protection law reveal important historical contrasts between India and the EU. These differences affected the clarity, predictability, and operationalization of legal obligations relevant to corporate actors.

In India, the recognition of privacy as a constitutional right emerged primarily through judicial interpretation. The Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India articulated privacy as intrinsic to life and liberty under Article 21.[61] This judgment provided a normative foundation for data protection but did not specify operational compliance standards for corporations. Judicially driven evolution tends to articulate broad principles, leaving detailed rule-making to subsequent legislative action.

Historically, this model produces normative depth but regulatory indeterminacy. Corporations may recognize the importance of privacy yet lack precise compliance benchmarks. As a result, integration into corporate governance can be slower, relying on future statutes or regulatory clarification.

The EU followed a different path. Data protection norms were codified through legislative harmonization, beginning with the 1995 Directive and culminating in the GDPR.[62] These instruments specified duties relating to lawful bases, data subject rights, accountability, and security. The Court of Justice of the European Union (CJEU) reinforced these norms through

interpretation but did not originate them.

Legislatively driven frameworks historically provide clearer operational guidance. Corporations can translate statutory requirements into internal compliance programs. This clarity facilitated earlier incorporation of data protection into risk management and due diligence processes. Thus, the EU‘s legislative leadership supported earlier corporate adaptation.

2.12. Merger Control Integration

Merger control in the EU developed as a supranational instrument designed to safeguard competition within the internal market. Council Regulation 4064/89 and later Regulation 139/2004 centralized review of concentrations with a Community dimension.[63] Transactions meeting turnover thresholds required prior notification and were subject to standstill obligations.

Historically, this meant that regulatory approval was not peripheral but integral to transaction completion. Corporate actors internalized the expectation that large transactions would be scrutinized for market effects. Due diligence therefore expanded to include competition analysis, market definition, and potential remedies.[64]

Although early merger control focused on traditional indicators such as market share and pricing power, the regulatory culture it fostered was significant. Firms became accustomed to viewing regulatory clearance as a transactional variable. When data later emerged as a source of competitive advantage in digital markets, this regulatory mindset facilitated its integration into competition analysis.

India introduced merger control later through the Competition Act, 2002.[65] Historically, Indian due diligence had already developed as a private-law exercise. Competition review was layered onto existing practice rather than forming its foundation. This sequencing influenced corporate perceptions: regulatory risk was initially seen as episodic rather than structural.

2.13. Recognition of Data as an Economic Resource

The EU‘s Database Directive marked a historically important recognition that investment in data

collection itself warranted legal protection.[66] The sui generis right protected substantial investment in obtaining or verifying database contents. This was not a property right in facts but a protection for structured data infrastructures.

This recognition influenced commercial behavior by signaling that data aggregation had independent economic value. Firms investing in large datasets particularly in telecommunications finance, and online services could treat these investments as legally protectable. In transactional contexts, databases began appearing in asset schedules and valuation analyses.

India did not create a comparable sui generis regime. Data protection relied on copyright in compilations, contract law, and confidentiality.[67] The absence of a dedicated framework meant doctrinal clarity remained limited. Commercial practice recognized value in data, but legal categories did not evolve in parallel.

2.14. Historical Impact on Modern Data Diligence

Modern data diligence is not a revolutionary legal invention; rather, it represents the incremental adaptation of traditional due diligence frameworks to a landscape where data processing is a regulated, legally significant activity. Historically, corporate due diligence was a localized exercise focused on verifying tangible asset ownership, quantifying financial liabilities, and assessing tax exposure. This classical model operated on the assumption that assets were discrete, easily transferable, and verifiable through formal titles of ownership.[68]

The maturation of data protection jurisprudence fundamentally disrupted this paradigm by introducing the concept of **compliance-dependent value**. Data assets can no longer be evaluated solely on their economic utility or physical possession; their legal "usability" is now contingent upon the lawful nature of their collection, processing, and retention. As regulatory regimes most notably in the EU attained institutional maturity, corporate actors recognized that non-compliant data practices could trigger significant post-transaction liabilities that diminish the overall value of an acquisition.[69]

One of the most observable historical shifts is the expansion of due diligence questionnaires. In

previous decades, these checklists prioritized intellectual property registrations and material contracts. Modern iterations, however, feature exhaustive inquiries into privacy policies, consent architectures, cross-border transfer mechanisms, and historical data breach records.[70] This evolution was not driven by theoretical foresight but was a reactive response to high-profile enforcement actions and evolving regulatory guidance. Consequently, data diligence developed as a cumulative practice rather than a product of a singular doctrinal redesign.

This shift is equally evident in the evolution of **Representations and Warranties**. Transactional documents now routinely include specific assurances regarding adherence to data protection statutes, the absence of pending regulatory investigations, and the maintenance of "reasonable" security standards.[71] Historically, these clauses have been modeled after environmental and labor law protections, signaling that data protection has moved from the realm of proprietary entitlement into the category of structural regulatory risk.

Risk allocation mechanisms have followed a similar trajectory. Indemnities covering data breaches or administrative fines are now standard in cross-border transactions involving EU-based entities.[72] The use of escrow accounts and price adjustments to account for anticipated compliance costs further demonstrates how corporate actors translate regulatory uncertainty into quantifiable financial terms. Disclosure practices have likewise matured; sellers are increasingly transparent regarding prior data incidents and cybersecurity measures, reflecting a broader historical movement toward transparency in highly regulated sectors.[73]

Ultimately, these modern developments were layered onto existing diligence frameworks rather than replacing them. Traditional models of asset verification persist, but they are now augmented by public-law regulatory inquiries. This layering explains the fragmented appearance of modern data diligence it is a hybrid of private law and public regulation. In a comparative sense, EU transactions integrated these practices earlier due to the "Brussels Effect" and higher enforcement visibility, while Indian transactions adopted them more gradually, often precipitated by exposure to international markets.[74]

2.15. Conclusion

The historical evolution of corporate, privacy, and intellectual property law reveals parallel yet largely independent developmental paths. Traditionally, corporate law prioritized the verification of ownership, the mechanics of risk allocation, and the maintenance of transactional certainty. Privacy law, meanwhile, focused on the preservation of human dignity, individual autonomy, and the right to informational self- determination. Intellectual property law sought to protect creative and inventive outputs through established proprietary models. None of these regimes were originally architected to accommodate assets that are non-rivalries, inherently compliance-dependent, and composite in nature.

The advent of data and AI systems disrupted these silos by challenging fundamental legal assumptions regarding exclusivity, control, and valuation. The economic worth of these digital assets is not derived merely from possession but is inextricably linked to their lawful provenance, regulatory history, and the sustainability of their governance models. Historically, legal systems have met this challenge through instrumentalism, stretching existing doctrines to cover new technological realities rather than engineering unified, purpose-built frameworks.

Consequently, the concept of data-centric due diligence emerged at the precarious intersection of corporate risk management and public-law accountability. This practice is historically contingent, defined by decades of doctrinal layering. Within the European Union, the early adoption of rights-based regulations embedded data compliance directly into corporate governance structures. In India, the constitutional recognition of privacy and subsequent statutory developments have gradually exerted similar pressures on the corporate sector.

Significantly, neither jurisdiction originally designed its due diligence frameworks for the unique needs of data-intensive enterprises. Contemporary transactional practices remain adaptations of tools initially forged for earlier economic contexts. Modern challenges ranging from the verification of training data provenance and inherited liability to algorithmic opacity and compliance sustainability are direct products of this historical evolution.

A rigorous understanding of this trajectory clarifies why existing diligence tools often appear

strained when applied to AI-driven enterprises. This tension is the result of a temporal mismatch: legal doctrines inevitably evolve at a slower pace than technological markets. Historical analysis, therefore, serves a dual purpose: it is both descriptive and explanatory. It reveals that modern data diligence is not a sudden doctrinal invention but a cumulative, adaptive response to a structural transformation in the very nature of corporate assets.

CHAPTER-III

CORPORATE AND LEGISLATIVE FRAMEWORK GOVERNING DATA PROTECTION AND AI ASSETS

3.1. Introduction: Scope, Objectives, and Corporate Centrality

This chapter provides a critical examination of the corporate and statutory frameworks governing data and artificial intelligence (AI) assets, with a primary comparative focus on India and the European Union (EU). It posits that data diligence in modern transactions transcends mere technical auditing or checklist-based compliance; rather, it constitutes a fundamental corporate law challenge shaped by fiduciary governance, enterprise liability, and statutory architecture. As data and AI systems evolve into value-defining assets, the legal regimes regulating their lifecycle increasingly dictate transactional risk profiles, valuation metrics, and deal structures.

The inquiry is strictly doctrinal and comparative, focusing on corporate legal implications and statutory adherence. It analyzes how data protection and AI-relevant norms are operationalized through corporate governance mandates, internal controls, and liability regimes. Furthermore, it explores the influence of these norms on Mergers and Acquisitions (M&A) mechanics, including the formulation of representations and warranties (R&Ws), indemnities, conditions precedent, and disclosure standards.

Corporate legal frameworks are central to data diligence for three foundational reasons:

i. **Entity-Centric Responsibility:** Data protection regimes attach obligations to legal entities (controllers/fiduciaries and processors) rather than isolated acts, embedding compliance into the core of corporate governance.
ii. **Enterprise Liability Models:** Administrative fines and compensation regimes convert compliance failures into significant financial exposures, directly impacting deal pricing.
iii. **Fiduciary Oversight:** Boards and senior management are under a fiduciary duty to implement systems capable of monitoring legal risks. Where AI is core to a business model, oversight failures may implicate directors' duties of care and internal controls.

3.2 Corporate Governance Interface: Data, AI, and Fiduciary Oversight

3.2.1 Entity-Centric Compliance and Board Oversight

Modern data protection regimes impose rigorous duties on legal entities that define the "purposes and means" of processing. In the EU, the General Data Protection Regulation (GDPR) establishes obligations grounded in accountability and documentation.[75] Core principlessuch as lawfulness, purpose limitation, and data minimizationfunction as continuous mandates rather than episodic rules. The accountability principle requires controllers to implement technical and organizational measures and, crucially, to maintain the capacity to demonstrate compliance to regulators.

This architecture necessitates the integration of compliance into the governance structure. The appointment of a Data Protection Officer (DPO), the execution of Data Protection Impact Assessments (DPIAs) for high-risk activities, and the maintenance of processing records are governance instruments that facilitate internal accountability and information flow.

In India, the Digital Personal Data Protection Act, 2023 (DPDP Act) adopts a similar accountability-based model by imposing obligations on ―Data Fiduciaries.‖[76] These include mandates for purpose specification, security safeguards, and breach notification. Significant Data Fiduciaries (SDFs) face heightened requirements, such as independent data audits. From a corporate law perspective, these statutory duties intersect with directors‘ duties of care, skill, and diligence. Failure to establish oversight mechanisms in data-intensive operations may expose boards to scrutiny for deficient risk management.

3.2.2 Internal Controls, Documentation, and Assurance

Data and AI compliance are inherently documentation-intensive. Records of lawful bases, consent logs, data processing agreements (DPAs), and breach registers create an auditable trail. In AI contexts, this extends to training data provenance and model validation protocols. These artefacts function as internal controls analogous to financial reporting controls. Their absence is not merely a technical flaw; it undermines the enterprise's ability to prove accountability, leading to heightened diligence burdens and expanded R&Ws in transactions.

3.3 Statutory Architectures and Corporate Obligations

3.3.1 European Union: GDPR as a Corporate Compliance Regime

The GDPR‘s corporate relevance is defined by its entity-centric design and substantial penalty framework. Controllers must adopt "data protection by design and by default," ensuring that privacy is integrated into the product lifecycle.[77] Joint and several liability, along with the right to compensation for material or non-material damage, converts compliance gaps into tangible financial risks. In M&A, particularly share acquisitions where the legal entity persists, liabilities may crystallize post-closing for pre-closing conduct, necessitating a deep dive into historical practices.

3.3.2 India: DPDP Act and Corporate Accountability

The DPDP Act structures corporate obligations around consent-based processing and data principal rights.[78] The Act‘s penalty framework signals that failures in consent management or vendor oversight can generate material financial exposure. For AI systems, training and deployment must align strictly with consent parameters and "legitimate uses" defined by the statute. This design shapes how enterprises structure data lifecycles and vendor relationshipsfactors that are directly relevant to transactional diligence.

3.4 Enterprise Liability and Risk Allocation

Enterprise liability in data law is designed to be "effective, proportionate, and dissuasive."[79] In the EU, administrative fines calibrated to global annual turnover ensure that data compliance remains a board-level risk calculation. Similarly, the Indian DPDP Act translates compliance failures into high-magnitude financial penalties. For AI systems, liability may also stem from automated decision-making that affects individuals' rights, requiring robust human oversight and redressal mechanisms.

In transactions, enterprise liability dictates deal mechanics. Buyers must assess the probability of sanctions and the cost of remediation, while sellers seek to mitigate exposure through thorough disclosure and negotiated limitations.

3.5 M&A Transaction Structuring Implications

3.5.1 Representations, Warranties, and Covenants

Diligence findings manifest in R&Ws covering compliance with relevant laws, the adequacy of security measures, and the lawful provenance of data. AI-specific warranties often focus on licensing compliance and model governance. Covenants may be utilized to mandate pre-closing remediation or post-closing integration steps.

3.5.2 Indemnities, Escrows, and Conditions Precedent

Where specific risks are identified, indemnities and escrows are employed to allocate financial responsibility. In certain high-risk scenarios, the completion of a data audit or the remediation of a security vulnerability may be set as a condition precedent to the closing of the transaction.

3.5.3 Integration and Governance Harmonization

Post-merger integration requires the reconciliation of divergent compliance frameworks. Harmonizing consent databases and security standards is a legal necessity to maintain the lawful status of data processing across the newly formed group. AI systems, when integrated across entities, require aligned governance to ensure consistent accountability and oversight.

3.6 Defining “Data Assets” and “AI Assets” in Corporate Law

Within the spheres of corporate governance and transactional practice, "assets" are broadly understood as resources under an enterprise's control from which future economic advantages are anticipated. Although corporate law lacks a singular, universal definition, both financial reporting standards and commercial custom identify control and the potential for economic benefit as the primary criteria for asset classification.[80] In the modern digital economy, data and artificial intelligence (AI) systems fulfill these requirements when they become indispensable to revenue generation, cost optimization, or the maintenance of competitive advantages.

A rigorous legal analysis must, however, distinguish between the mere exercise of control and the privilege of lawful usability. Data protection statutes condition the legitimate utilization of personal information upon adherence to strict regulatory mandates. Consequently, the "asset value" of data is inextricably linked to an enterprise‘s ability to demonstrate compliance with

principles of lawfulness, purpose limitation, and robust security protocols.[81] This conditionality does not strip these resources of their status as assets; rather, it reconfigures the metrics of valuation and risk. From a corporate perspective, data and AI are "compliance-dependent assets," as their economic utility is fundamentally mediated by their regulatory standing.

"Data assets" encompass datasets and information resources over which a firm exerts control to derive economic gain, bounded by legal restrictions concerning collection, processing, and retention. This category includes customer repositories, behavioral analytics, and curated datasets utilized for model training. Where these resources are protected by contractual stipulations, trade secret doctrines, orwithin the European Union*sui generis* database rights, they manifest distinct legal attributes of property.[82]

Conversely, "AI assets" denote algorithmic systems and model-related resources employed for tasks such as classification, prediction, or generation. Legally, AI assets are composite entities, integrating software code, model parameters, validation datasets, and operational governance frameworks. Their various elements may be protected through a mosaic of copyright (for code), trade secrets (for weights and architecture), and contract law (for licensing).[83] Their character as assets is derived from the enterprise's ability to control and reproduce them to create value. Thus, corporate law must view data and AI not as monolithic objects, but as bundles of rights and obligations.

3.6.1 *Taxonomy: Personal Data, Non-Personal Data, Proprietary Datasets, Algorithms, and Trained Models*

a) Personal Data Under the General Data Protection Regulation (GDPR), "personal data" extends to any information concerning an identified or identifiable natural person.[84] This expansive definition ensures that personal data is not a freely tradable commodity; its processing must be anchored in a valid legal basis and remain subject to the rights of data subjects.[85] In corporate terms, personal data is a relational asset; its value is constrained by the necessity of ongoing governance rather than classical proprietary ownership.

The Indian Digital Personal Data Protection Act (DPDP Act) similarly regulates "digital personal data," framing processing around consent and specified legitimate uses.[86] The

fiduciary model adopted in India emphasizes the obligations of the "Data Fiduciary" over ownership claims, making asset value contingent upon the integrity of the compliance framework.

b) Non-Personal Data Non-personal data (NPD) consists of anonymized or industrial datasets that fall outside the scope of personal privacy regimes. While NPD is subject to fewer statutory hurdles, it remains influenced by contractual and competition law constraints. Corporate actors often view NPD as a strategic asset, yet legal risks persist, particularly regarding the potential for re-identification or the complexities of "mixed" datasets.[87]

c) Proprietary Datasets and Databases In the EU, the Database Directive provides a dual layer of protection: copyright for creative selection or arrangement, and a *sui generis* right for databases representing a substantial investment in data verification or presentation.[88] This formalizes the asset-like nature of data compilations. India, lacking a *sui generis* regime, relies on copyright in "compilations" and the law of contracts to preserve database value, placing significant weight on physical security and restrictive covenants.[89]

d) Algorithms and Software Algorithms implemented through code are protected as computer programs under copyright law in both the EU and India.[90] Because copyright protects the expression of the code rather than the underlying functional idea, enterprises frequently utilize escrow agreements and licensing to maintain control. In M&A, diligence must rigorously verify the chain of title and open-source obligations to mitigate deployment risks.

e) Trained Models and Model Weights The protection of trained modelswhich embody statistical representations learned from datatypically resides in trade secrets and contract law, given that model weights are often viewed as functional parameters rather than creative expressions.[91] The value of these assets depends heavily on the "lawful provenance" of the training data. If the underlying data was obtained unlawfully, the downstream deployment of the model faces significant legal exposure.

3.6.2 *Why Data and AI Qualify as Corporate Assets*

Three doctrinal pillars support the classification of these resources as corporate assets:

1. **Control and Legal Excludability:** Enterprises exert control via trade secret regimes, encryption, and confidentiality agreements. These legal "walls" allow firms to exclude others from the resource's commercial value.[92]
2. **Economic Benefit Expectations:** These systems drive revenue through personalization and cost reduction through automation. Modern corporate finance recognizes these as "identifiable intangibles" when future benefits are probable.[93]
3. **Transactional Transferability:** While personal data is not "owned" in the traditional sense, the right to process datasets and the ownership of software licenses are transferable. In "share deals," the entire compliance history of the entity transfers to the acquirer, further supporting asset treatment.

The essential caveat remains: asset quality is fundamentally a reflection of regulatory hygiene. Unlawful collection or security lapses do not just create liability; they impair the asset's very usability. Consequently, data and AI are best understood as "regulated intangibles"valuable resources whose commercial utility is strictly bounded by their legal architecture.

3.7 Digital Personal Data Protection Act, 2023: Corporate and Transactional Implications

3.7.1 Statutory Positioning and Corporate Relevance

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents the inaugural comprehensive legislative framework governing the processing of digital personal data in India. Structurally, the enactment is entity-centric; obligations are anchored to "Data Fiduciaries" and "Data Processors," effectively embedding compliance mandates within the internal corporate governance and operational controls of the enterprise.[94] By design, the statute elevates personal data processing from a private, bilateral contractual matter between firms and individuals to a strictly regulated corporate function. This shift is particularly consequential for Mergers and Acquisitions (M&A) because liabilities, documentation requirements, and remediation duties attach to the legal entity, persisting through changes in ownership.

The jurisdiction of the Act extends to the processing of digital personal data within Indian territory, as well as extraterritorial processing conducted in connection with the offering of goods or services to individuals within India.[95] This broad nexus necessitates that multinational groups

evaluate their exposure based on data flows and processing activities rather than mere physical presence. Consequently, transactional diligence must move beyond a territorial assessment to a functional analysis of the data processing nexus.

The corporate significance of the DPDP Act is derived from three primary characteristics:

- An **accountability-based architecture** necessitating demonstrable compliance.
- A **consent-centric model** supplemented by narrowly defined "legitimate uses."
- A **stringent penalty framework** designed to generate material financial consequences.

3.7.2 Data Fiduciary Obligations and Governance Architecture

The DPDP Act mandates that Data Fiduciaries adhere to baseline duties, including ensuring the lawfulness of processing, purpose limitation, and the implementation of "reasonable security safeguards" to prevent data breaches.[96] These obligations are continuous and system-dependent, requiring the institution of risk-based technical and organizational measures calibrated to the scale and nature of the data.[97]

From a corporate law perspective, these statutory mandates intersect with the fiduciary duties of directors. Under the Companies Act, 2013, directors are required to exercise due and reasonable care and act in the best interests of the company.[98] Where data processing is central to an enterprise‘s value proposition, a failure to institute adequate safeguards may result in foreseeable liabilities and reputational damage, thereby engaging board- level oversight responsibilities. Furthermore, the requirement to notify both the Data Protection Board and affected individuals of any personal data breach necessitates robust incident detection and response mechanisms.[99] In the context of a transaction, the maturity of these response protocols serves as a critical diligence item for risk pricing.

3.7.3 Consent Architecture and Corporate Systems

Consent under the DPDP Act is valid only if it is free, specific, informed, unconditional, and manifested through a clear affirmative action.[100] Accompanied by a mandatory notice describing the data and the purpose of its use, this framework compels enterprises to implement sophisticated

consent management systems.[101] For a corporation, consent is an operational system rather than a static administrative requirement; it must be synchronized with product design, marketing workflows, and vendor arrangements.

While the Act recognizes certain "legitimate uses" that bypass the need for explicit consent, the dependence on valid consent remains a primary concern for AI-driven enterprises.[102] If datasets utilized for training AI models exceed the scope of the original disclosure, their lawful usability may be compromised. During M&A, acquirers must meticulously examine consent logs and notice templates to ensure that the legal basis for processing remains intact post-acquisition.

3.7.4 Significant Data Fiduciary (SDF) Classification

The Central Government reserves the authority to designate certain entities as "Significant Data Fiduciaries" (SDFs) based on variables such as data volume, sensitivity, and the potential risk to the rights of individuals or national integrity.[103] SDFs are burdened with heightened governance obligations, including the mandatory appointment of a Data Protection Officer (DPO) and the conduct of independent data audits.[104]

For acquirers, SDF status signals an increased cost of compliance and greater regulatory visibility. Conversely, for a target nearing the threshold of such a designation, transactions must account for the necessary future investment in compliance infrastructure.

3.7.5 Compliance Burdens and Documentation

Corporate compliance under the Act is multi-layered, involving vendor oversight through processor contracts, data minimization, and retention controls aligned with the stated purpose.[105] Processor arrangements require specific contractual protections and processing instructions, forming part of the enterprise‘s wider compliance perimeter. Documentation serves as the primary evidence of "demonstrable compliance." The absence of comprehensive policies, training records, and logs increases transactional uncertainty, often leading to more conservative valuations or the imposition of escrow structures.

3.7.6 Framework and Enterprise Liability

The DPDP Act introduces a schedule of monetary penalties calibrated to the gravity of the

contravention, with high upper limits for failures relating to security safeguards and breach notification.[106] Enterprise liability is not limited to intentional misconduct; systemic negligence can trigger substantial sanctions. In share-based M&A, these liabilities attach to the continuing entity, necessitating the use of targeted indemnities to allocate risk between the parties.

3.7.7 Impact on Corporate Governance and Board Oversight

The statutory design pulls data governance into the boardroom, treating it as a primary operational risk. Boards may utilize specialized committees and periodic audits to satisfy their duties of diligence. While the Act does not create director-specific penalties, it establishes enterprise obligations whose breach can severely impair corporate interests. Transactional acquirers increasingly view governance maturity as a reliable proxy for the long-term sustainability of the target's business model.

3.7.8 Relevance in M&A Due Diligence and Valuation

The DPDP Act fundamentally reconfigures the parameters of diligence and valuation:

- **Lawful Usability:** The economic utility of datasets is contingent upon valid consent and purpose alignment.
- **Vendor Ecosystems:** Processor and sub-processor chains expand the scope of the diligence perimeter.
- **SDF Trajectory:** Potential future obligations for high-growth firms alter cost structures.
- **Integration Complexity:** Post-merger harmonization of divergent consent frameworks is legally required for operational continuity.

These factors inform the broader deal architecture, resulting in more granular representations and warranties, conditions precedent, and post-closing covenants.

3.8 The Information Technology Act, 2000

3.8.1 Statutory Positioning and Corporate Relevance

The Information Technology Act, 2000 (IT Act) serves as the foundational, albeit pre-comprehensive, legislative framework for India's digital economy. Despite the subsequent introduction of more specific privacy mandates, the IT Act retains its centrality in governing

corporate data handling, cybersecurity protocols, and the liability of digital platforms. Its significance within corporate law is predominantly concentrated in three spheres:

i. the establishment of civil liability for deficiencies in data protection;
ii. the formal statutory recognition of "reasonable security practices"; and
iii. the regulation of intermediary liability, which dictates the governance and risk allocation strategies of digital platforms.[107]

For corporate entities, the IT Act functions as a mechanism that converts technical or systemic failures into tangible legal exposure. A critical provision in this regard is Section 43A, which mandates compensatory liability for body corporates that handle "sensitive personal data or information" (SPDI). If such an entity is found negligent in implementing or maintaining reasonable security standards, resulting in wrongful loss or gain, it becomes liable for damages.[108]This provision effectively embeds a negligence- based standard into the bedrock of corporate risk management, incentivizing the adoption of documented and verifiable security programs. During mergers and acquisitions (M&A), Section 43A exposure necessitates rigorous due diligence concerning a target‘s security architecture, audit trails, and the maturity of its incident response protocols.

3.8.2 *SPDI Rules and Cybersecurity Obligations*

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) provide the operational framework for Section 43A. These rules define SPDI to include sensitive categories such as financial data, health records, and biometric information, while imposing requirements for privacy policies and explicit consent for data collection.[109] Notably, the rules recognize international standards, such as ISO/IEC 27001, as benchmarks for demonstrating compliance with the "reasonable security" mandate.[110]

From the perspective of corporate governance, the SPDI Rules establish a clear set of expectations regarding internal controls: the publication of privacy policies, the maintenance of consent artifacts, the enforcement of purpose limitation, and the appointment of a Grievance Officer.[111] These requirements function as internal controls analogous to compliance mandates in other regulated sectors. Because these rules apply specifically to "body corporates," they emphasize enterprise-level accountability over individual conduct.

Furthermore, cybersecurity obligations are reinforced by the directions issued by the Computer Emergency Response Team–India (CERT-In) under Section 70B of the Act. The 2022 Directions introduced stringent mandates, including the reporting of cyber incidents within six hours, mandatory log retention, and heightened coordination with authorities.[112] For acquirers, a target's historical adherence to CERT-In directives serves as a primary indicator of its governance maturity and regulatory standing.

3.8.3 Intermediary Liability and Platform Governance

Sections 79 and 69A of the IT Act delineate the "safe harbor" protections and government blocking powers applicable to intermediaries. Section 79 provides conditional immunity to platforms for third-party content, provided they observe prescribed due diligence and remove unlawful material upon receiving "actual knowledge" or legal orders.[113] This framework has been further refined by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which impose heightened compliance burdens on "significant social media intermediaries."[114]

For technology-driven enterprises, these rules necessitate the integration of compliance officers and nodal contacts into their corporate structure. These roles are essential for internal escalation and content moderation. Judicial scrutiny has further shaped this domain; in *Shreya Singhal v. Union of India*, the Supreme Court interpreted "actual knowledge" to mean knowledge received via court orders or government notifications, thereby mitigating the burden of proactive monitoring while preserving compliance duties.[115] Conversely, in *Google India Pvt Ltd v. Visaka Industries*, the Court reiterated that safe harbor protection is conditional and contingent upon specific factual circumstances.[116]

3.8.4 Corporate Exposure and Compliance Risk

The IT Act creates a multi-layered risk profile for enterprises, spanning civil compensation, criminal penalties for cyber offences (such as those under Sections 66C through 66E), and regulatory compliance. In the context of M&A, buyers must evaluate:

- Security certifications and the results of independent audits.
- Historical breach records and the efficacy of subsequent remediation.

- Adherence to "safe harbor" due diligence for intermediaries.
- The nature of past correspondence with regulatory bodies like CERT-In.

Because Section 43A liability hinges on the concept of negligence, the presence of a robust, documented security program is often the deciding factor in mitigating risk. Entities that lack such systems frequently face valuation discounts or more stringent indemnity and escrow requirements in transaction documents.

3.9 Allied Corporate Law Obligations

3.9.1 Duties of Directors and Oversight of Data Governance

Under the Companies Act, 2013, directors are bound by fiduciary duties to act in good faith and with due and reasonable care, skill, and diligence.[117] While these duties are not explicitly framed in terms of data, they encompass the oversight of all material risks that could affect corporate interests. In data-intensive enterprises, the failure to implement reasonable oversight of data protection and cybersecurity may be interpreted as a breach of these duties if it leads to foreseeable and significant legal exposure. Board-level involvement typically manifests through risk committees and periodic management reporting on information security.

3.9.2 Disclosure Obligations and Material Information

Securities regulations necessitate the accurate and timely disclosure of "material" events. Significant data breaches or regulatory investigations often meet the materiality threshold for listed entities under the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.[118] For M&A transactions involving listed companies, any discrepancy between a target's internal incident logs and its public disclosures represents a substantial legal and reputational risk.

3.9.3 Risk Management and Internal Controls

Section 134 of the Companies Act requires the Board‘s Report to provide a statement on the implementation of risk management policies.[119] For data-driven firms, cybersecurity is increasingly classified as a risk that may threaten the company's "existence." Furthermore, internal financial controls often overlap with IT general controls (ITGCs) and access management systems. Documented evidence of tested controls and remediation efforts is therefore essential for both

regulatory compliance and transactional due diligence.

3.9.4 ESG and Data Governance Intersections

The "G" (Governance) pillar of Environmental, Social, and Governance (ESG) frameworks now frequently includes data privacy and security. The Business Responsibility and Sustainability Report (BRSR) framework in India requires listed entities to disclose their governance practices, which may encompass data protection metrics.[120] As investor scrutiny of data ethics intensifies, governance quality in this area has become a significant factor in valuation and the ease of post-merger integration.

3.10 Statutory and Regulatory Framework: The European Union

3.10.1 GDPR Corporate Implications

i. Conroller–Processor Allocation and Corporate Structuring

The architecture of the General Data Protection Regulation (GDPR) is predicated upon the fundamental distinction between "controllers"entities that establish the purposes and means of data processingand "processors"those acting strictly on behalf of the controller.[121] This classification is far from a mere administrative exercise; it dictates the structural design of corporate compliance, the allocation of contractual risk, and the internal governance of corporate groups. Controllers bear the primary burden for upholding the principles enshrined in Article 5 and must maintain the capacity to prove such adherence under the principle of accountability.[122] Conversely, processors are subject to direct statutory mandates, including the implementation of rigorous security measures and the maintenance of processing logs, and face direct liability for breaches of duties specifically assigned to them.[123]

Within corporate conglomerates, this role allocation necessitates a granular mapping of data flows between various affiliates and third-party vendors. The concept of "joint controllership" under Article 26 further requires a transparent arrangement that delineates the respective responsibilities of each entity, which must be communicated clearly to the data subjects.[124] In the context of Mergers and Acquisitions (M&A), due diligence must rigorously verify whether these role designations align with operational realities. Any misclassification can result in the unforeseen transfer of liability to the acquirer upon

closing. Consequently, transaction documents invariably include representations and warranties (R&Ws) to confirm accurate role allocation and the existence of compliant Data Processing Agreements (DPAs) as mandated by Article 28.[125]

ii. Accountability Principle as a Governance Mandate

The GDPR‘s accountability principle represents a shift from passive compliance to active demonstration.[126] This mandate integrates documentation and internal auditing directly into the bedrock of corporate governance. Records of Processing Activities (RoPAs), "privacy by design" policies, training modules, and incident response protocols are transformed from technical files into essential governance artifacts.[127]

From a corporate law perspective, accountability serves as a sophisticated internal control system for managing legal risk. Boards and executive management are tasked with ensuring that reporting lines and resources are sufficient to sustain continuous compliance. In specific instancessuch as large-scale monitoring or the processing of special categories of datathe appointment of a Data Protection Officer (DPO) is required.[128] The DPO serves as an independent governance node with direct access to senior management, thereby institutionalizing the oversight of data-related risks. For transactional purposes, the existence of a mature accountability framework acts as a proxy for compliance sustainability; its absence frequently leads to valuation adjustments or the imposition of post-closing covenants.

iii. DPIAs and Structured Risk Assessment

Data Protection Impact Assessments (DPIAs) are mandatory for processing activities identified as "high risk" to the rights and freedoms of individuals, such as systematic profiling or large-scale processing of sensitive datasets.[129] DPIAs are dynamic decision records that evidence a corporation‘s deliberation regarding risk mitigation.

Enterprises utilizing data-intensive analytics or artificial intelligence (AI) frequently trigger these requirements. Guidance from the European Data Protection Board (EDPB) clarifies that the adoption of novel technologies often necessitates such assessments.[130] During M&A, diligence teams must verify that DPIAs were conducted where required, that proposed mitigation strategies were actually implemented, and that supervisory authorities were consulted in cases where residual high risks persisted.[131]

iv. Administrative Fines and Enterprise Liability

The GDPR empowers supervisory authorities to impose significant administrative fines, calibrated based on the gravity and duration of the infringement, with potential ceilings linked to a company's global annual turnover.[132] This regime is explicitly designed to be "effective, proportionate, and dissuasive."[133] Liability is strictly enterprise-centric; sanctions are leveled against the legal entity and may be accompanied by corrective orders, such as processing bans.[134]

For M&A, this fine regime converts abstract compliance into quantifiable financial exposure. In share-based acquisitions, historical infringements remain with the target entity, potentially crystallizing post-closing. Therefore, buyers meticulously scrutinize breach histories and regulatory correspondence, utilizing indemnities and escrows to shield against identified risks.

v. Implications for Corporate Governance

In data-driven industries, GDPR compliance has ascended to a board-level priority. Effective governance requires the establishment of clear accountability structures, ensuring the independence of the DPO, and the integration of privacy concerns into product development pipelines. While the GDPR does not impose specific personal liability on directors, the significant potential for operational disruption and financial sanctions places data governance squarely within the fiduciary remit of oversight.

3.10.2 *EU Regulatory Approach to AI Assets*

i. Datasets, Automated Systems, and Algorithmic Decision-Making

Under the GDPR, datasets utilized in AI systems remain subject to the core principles of lawfulness and purpose limitation, regardless of the sophistication of the technology.[135] Article 22 specifically regulates automated decision-making and profiling, granting individuals the right to contest decisions that produce "legal or similarly significant effects" based solely on automated processing.[136] This necessitates that corporations maintain human-in-the-loop safeguards and the ability to explain the logic behind algorithmic outputs. Entities deploying AI must ensure that the training and validation of models align with the original lawful bases for data collection; repurposing existing datasets for AI development often requires a fresh assessment of purpose compatibility.[137]

ii. Compliance Burdens for Corporate AI Deployment

Corporate compliance in AI deployment is defined by transparency and rigorous documentation. DPIAs are standard for AI use cases involving large-scale profiling. Furthermore, transparency obligations require that firms provide intelligible information regarding the logic of their processing activities.[138] The security of the entire model pipelinefrom data stores to deploymentmust be ensured. This involves a complex vendor ecosystem (e.g., cloud providers and data annotators) that must be governed by Article 28-compliant DPAs.

The recent adoption of the EU AI Act adds a further layer of risk-based obligations for "high-risk" AI systems, including mandates for technical documentation and post-market monitoring.[139] While the AI Act targets systemic risks, the GDPR remains fully operative for any personal data processed by these systems, resulting in a cumulative regulatory burden for corporations.

iii. Interaction Between Data Protection and AI Regulation

The intersection of the GDPR and AI-specific legislation creates a multifaceted compliance landscape focused on data governance, transparency, and safety. While the GDPR protects individual rights, AI regulation prioritizes the safety and reliability of the system itself. For enterprises, this requires a coordinated compliance function that manages both silos. In M&A transactions, diligence must extend beyond basic data protection to include AI governance maturity, bias mitigation efforts, and the provenance of training datasets.

3.11 Corporate Governance Dimension

3.11.1 Board Responsibility for Data Governance

The elevation of data and artificial intelligence (AI) systems to the status of primary value-drivers has fundamentally repositioned data governance from a peripheral operational task to a core function of board-level oversight. While modern corporate law does not typically prescribe "data governance" as a standalone statutory duty for directors, it interprets such oversight through the expansive prism of fiduciary obligations, specifically the duties of care, diligence, and the mandate to act in the best interests of the company. Where the processing of personal information and the deployment of AI are intrinsic to an enterprise's commercial model, the foreseeable legal and

financial consequences of data mismanagement or regulatory breaches necessitate that boards treat data governance as a critical pillar of enterprise risk management.

In the Indian legal landscape, Section 166 of the Companies Act, 2013, requires directors to exercise due and reasonable care, skill, and diligence.[140] Consequently, when data protection and cybersecurity risks attain materiality, they fall squarely within the spectrum of risks that a prudent board is expected to mitigate. This expectation is further reinforced by the statutory requirement for boards to formulate and implement robust risk management policies.[141] Although the Companies Act remains technology-neutral, the logic of fiduciary oversight dictates that boards must proactively manage data governance, as failures in this domain can lead to punitive penalties, protracted litigation, and severe reputational impairment.

Within the European Union, the General Data Protection Regulation (GDPR) indirectly structures board oversight by attaching high-magnitude administrative fines and corrective measures to the legal entity itself.[142] Given that sanctions may reach a significant percentage of global annual turnover, data protection compliance has become a matter of financial materiality. This financial exposure necessitates board intervention as part of standard risk governance. Furthermore, the GDPR's "accountability principle" requires that compliance be demonstrable, implying that corporate leadership is responsible for ensuring the existence of verifiable policies, internal controls, and clear reporting lines.[143]

It is essential to note that the board‘s role is supervisory rather than executive; directors are tasked not with daily compliance management but with ensuring that systems are in place to monitor, escalate, and remediate data-related risks. A failure to institute such systems, particularly where risks are manifest, may expose the entity to avoidable liabilities and invite scrutiny regarding the adequacy of board oversight. The doctrinal anchor remains the fiduciary duty, now increasingly operationalized through the lens of digital risk.

3.11.2 *Role of Compliance Officers and Data Protection Officers*

The institutionalization of data governance within the corporate hierarchy is primarily achieved through specialized compliance roles. Under the GDPR, the designation of a Data Protection Officer (DPO) is mandatory for public authorities and entities involved in large-scale systematic monitoring or the processing of sensitive data categories.[144] The DPO is required to possess expert knowledge, maintain a significant degree of independence, and report directly to the highest levels

of management.[145]

Functionally, the DPO serves as a structured interface between the corporation and regulatory bodies, advising on compliance, monitoring adherence to laws, and guiding Data Protection Impact Assessments (DPIAs).[146]From a governance perspective, the DPO acts as a control function comparable to internal audit or compliance roles in the financial sector. The statutory protection ensuring that a DPO cannot be penalized for performing their duties underscores the importance of functional independence.[147]

The Indian Digital Personal Data Protection Act, 2023, similarly contemplates the appointment of a Data Protection Officer for "Significant Data Fiduciaries."[148] While the legislative architecture differs from the European model, the underlying rationale is identical: the centralization of accountability and the creation of a formal regulatory liaison. These roles are further supplemented by grievance officers under the SPDI Rules and compliance officers under intermediary guidelines.[149]

In the context of Mergers and Acquisitions (M&A), the seniority and resourcing of these compliance roles are vital diligence indicators. A well-integrated compliance function suggests governance maturity, whereas a nominal appointment lacking operational capacity may signal systemic fragility. The legal significance lies in the demonstrable effectiveness of the compliance architecture rather than mere formal titles.

3.11.3. Internal Controls and Audit Mechanisms

Data governance is operationalized through a network of internal controls and audit mechanisms designed to prevent, detect, and correct compliance failures. These controls encompass diverse areas such as access management, vendor due diligence, data retention schedules, and incident response protocols.

Under the Companies Act, 2013, directors must affirm the adequacy and effectiveness of "internal financial controls."[150] While traditionally focused on financial reporting, modern corporate practice increasingly integrates information technology (IT) and security controls within this environment, recognizing that data breaches can have profound financial reporting implications. Within the GDPR framework, Article 32 mandates that entities implement appropriate technical and organizational measures, including encryption and regular testing of system resilience, to ensure a level of security appropriate to the risk.[151]

Internal audit functions are increasingly tasked with conducting privacy and cybersecurity audits. The resulting documentation is critical for both regulatory defense and transactional due diligence. For an acquirer, audit findings and subsequent management responses provide deep insight into a target‘s risk posture. Conversely, the absence of a systematic audit trail often results in higher uncertainty and potential valuation discounts.

3.11.4. Data as Part of Fiduciary Risk Oversight

The integration of data governance into fiduciary oversight reflects the evolution of data into an asset that is as risk-laden as it is valuable. Fiduciary oversight has traditionally addressed financial and legal risks; data-related exposuresranging from regulatory fines to operational paralysisnow fit comfortably within this paradigm.

This is not a creation of new fiduciary duties, but a recognition that data-intensive operations have fundamentally altered the firm's risk profile. When AI systems influence core products, algorithmic bias or errors can trigger substantial legal consequences. While corporate law does not require directors to be technical experts, it does demand that they remain sufficiently informed to exercise meaningful oversight. This often involves a reliance on expert briefings, specialized committee structures, and formal escalation protocols.

In M&A, this oversight shapes the diligence narrative. Buyers assess whether data governance is truly embedded in the enterprise risk management framework. Sellers who can demonstrate a robust, board-led oversight framework are better positioned to provide credible representations and warranties regarding their compliance culture. In sum, data governance serves as the connective tissue between statutory mandates and transactional risk management.

3.11.5. Impact on Mergers & Acquisitions

The integration of data protection and artificial intelligence (AI) governance into Mergers and Acquisitions (M&A) practice signifies a structural transformation in the assessment of corporate value and risk. While traditional diligence prioritized tangible assets and registered intellectual property, contemporary transactions increasingly treat regulatory compliance, data provenance, and algorithmic integrity as the primary determinants of enterprise value. This shift is driven by the entity-centric nature of modern data regimes, which anchor liabilities to corporate actors and allow regulatory exposures to crystallize long after a transaction concludes. In this framework,

M&A structuring serves as a vital mechanism for the allocation of regulatory risk and the preservation of the "lawful usability" of digital assets.

3.12 Data Protection Due Diligence Checklists

Data protection due diligence has matured into a specialized workstream that bridges legal and technical inquiry. Its objective transcends the mere cataloging of information; it seeks to determine whether personal data was harvested and processed in accordance with statutory mandates and whether existing compliance architectures can sustain lawful utilization following the change in control.

Under the General Data Protection Regulation (GDPR), diligence exercises typically scrutinize Records of Processing Activities (RoPAs), the validity of lawful bases, consent management systems, and cross-border transfer protocols.[152] Given the mandate for "demonstrable compliance" under the accountability principle, documentation serves as the primary evidentiary artifact.[153] Furthermore, where high-risk processing is present, the existence and qualitative adequacy of Data Protection Impact Assessments (DPIAs) undergo rigorous review.[154]

In the Indian context, diligence encompasses adherence to the Digital Personal Data Protection Act, 2023, the SPDI Rules, and cybersecurity mandates under the IT Act. This involves a comprehensive review of privacy notices, security certifications, and incident response frameworks.[155] Notably, because Section 43A of the IT Act establishes a negligence-based standard for compensation, the perceived adequacy of security governance directly influences valuation.[156] For AI-driven targets, this inquiry expands to include dataset provenance and licensing compliance, acknowledging that the commercial viability of a proprietary model is entirely contingent upon the legality of the underlying data processing.

3.12.1 Representations and Warranties Relating to Data

Representations and warranties (R&Ws) function as the primary contractual tools for risk allocation. In data-intensive deals, these provisions specifically address the target's history of compliance, the absence of undisclosed security breaches, and the legal validity of its data collection and transfer mechanisms.

Standard R&Ws now include assertions that the target has implemented "reasonable security safeguards" and has not been the subject of regulatory investigations or notices. Within GDPR-influenced practice, these may extend to warranties regarding the mandatory appointment of a Data Protection Officer (DPO).[157] For AI assets, R&Ws increasingly cover the lawful sourcing of training data and the absence of third-party infringement claims. While these clauses do not bind public regulators, they serve as a private-law response to public-law obligations, effectively shifting the financial burden of regulatory defects between the buyer and the seller.

3.12.2 *Indemnities and Escrow Structures*

Indemnities are utilized to address identified risks where the precise financial impact remains uncertain. Data-specific indemnities often cover regulatory fines, remediation expenses, and losses resulting from third-party claims or data breaches. To provide financial security for these claims, parties frequently employ escrow arrangements or "holdbacks."

The negotiation of these indemnities is particularly complex in the EU, where GDPR fines may be linked to global turnover.[158] While the insurability or indemnification of administrative fines varies by Member State on public policy grounds, parties typically structure these protections around the collateral losses associated with such fines. Similarly, in India, the potential for significant penalties under the DPDP Act has made escrow structures a standard feature of deal architecture. These mechanisms reflect the temporal reality that data liabilities often surface well after the closing date.

3.12.3 *Compliance and Valuation of Data/AI Assets*

The compliance status of an enterprise now exerts a direct influence on its valuation. The economic utility of a dataset is not absolute; it is "compliance-dependent." If information was collected without valid consent or utilized beyond its disclosed purpose, its commercial exploitation may be legally restricted or prohibited under the principle of purpose limitation.[159]

For AI systems, the value of a model is inextricably linked to the legality of its training data and the sustainability of its governance. If a model is found to rely on improperly licensed or unlawfully sourced data, the requirement to retrain or decommission the system can lead to a substantial reduction in asset value. Valuation professionals, therefore, incorporate these regulatory risks through price adjustments, contingent consideration, or "earn-outs."[160]

3.12.4 *Ownership and Transferability Issues*

Doctrinally, data protection law does not recognize "ownership" of personal data in the classical proprietary sense; it regulates rights of processing and obligations of protection.[161]Consequently, in asset-based transactions, the transfer of datasets must be meticulously aligned with existing lawful bases and notice requirements. Consent granted to an original controller may not automatically transfer to a new entity if the underlying purposes of processing undergo a material change.[162]

In share-based transactions, the legal entity remains the "controller" or "fiduciary," ensuring greater continuity; however, post-closing integration may still trigger fresh compliance obligations if data flows are altered. For non-personal or proprietary data, transferability is governed by a combination of contract law, trade secrets, and intellectual property rights, such as the *sui generis* database rights in the EU.[163] The fundamental implication is that data assets are not "freely alienable" in the manner of tangible property; their transfer is a highly regulated process that prioritizes the continuity of lawful processing over the mere transfer of title.

3.13 Enterprise Liability

Enterprise liability regarding data and AI assets represents the convergence of regulatory design, private law exposure, and market discipline. Modern data protection regimes shift the focus from individual errors to entity-level obligations, anchoring liability to the corporate person. For corporations engaged in data-intensive or AI-enabled activities, this exposure becomes a structural component of enterprise risk and, consequently, a primary factor in transactional valuation.

3.13.1 *Regulatory Penalties*

Regulatory penalties constitute the most visible form of enterprise liability. Under the GDPR, supervisory authorities may impose administrative fines of up to €20 million or 4% of an undertaking‘s total worldwide annual turnover, whichever is higher.[164] The Court of Justice of the European Union (CJEU) has clarified that the concept of an "undertaking" must be interpreted in line with EU competition law, essentially viewing a corporate group as a single economic unit.[165] This means a parent company may be held liable for the infringements of its subsidiaries if it exerts decisive influence over them, significantly elevating the risk profile for multinational conglomerates.

In India, the Digital Personal Data Protection Act, 2023 (DPDP Act) establishes a schedule of financial penalties for specific contraventions, such as the failure to implement "reasonable security safeguards," with fines reaching up to ₹250 crore per instance.[166] While the DPDP Act departs from the GDPR's turnover-based model in favor of a per-violation ceiling, it maintains a strictly corporate-level focus for financial accountability. Furthermore, the Information Technology Act, 2000 continues to provide for compensation where corporate negligence in maintaining security practices results in "wrongful loss or gain."[167]

3.13.2 *Civil Liability Exposure*

Civil liability operates as a parallel track to regulatory enforcement. Article 82 of the GDPR grants any person who has suffered "material or non-material damage" the right to seek compensation directly from the controller or processor.[168] In the landmark *Österreichische Post* case, the CJEU confirmed that while a mere infringement of the GDPR does not automatically grant a right to compensation, there is no "seriousness threshold" for non-material harm; even *de minimis* emotional distress may be compensable if proven.[169]

In the Indian context, civil exposure has traditionally been governed by Section 43A of the IT Act, which creates a negligence-based compensation regime.[170] Although the DPDP Act introduces a more comprehensive administrative framework, the potential for representative actions and consumer-led litigation remains a potent threat to corporate balance sheets. For M&A practitioners, civil liability represents a contingent risk that may surface years after a transaction, necessitating robust indemnity and escrow protections.

3.13.3 *Reputational and Shareholder Risk*

Reputational harm functions as a quasi-legal liability that often exceeds the value of regulatory fines. Data breaches can erode consumer trust, trigger mass attrition, and permanently impair brand equity. For listed entities, such events qualify as "price- sensitive information" requiring disclosure under securities regulations like SEBI's LODR.[8][171]Moreover, significant governance failures can lead to derivative litigation where shareholders allege that directors breached their fiduciary duties by failing to oversee material digital risks.

3.14 Comparative Analysis: India vs. European Union

Feature	European Union (GDPR)	India (DPDP Act / IT Act)
Liability Basis	Turnover-based (up to 4% global).	Per-violation ceiling (up to ₹250 cr).
Enterprise Concept	Focus on "Economic Unit" (Undertaking).	Focus on "Data Fiduciary" (Legal Entity).
Enforcement	Mature; high-profile, coordinated fines.	Nascent; institutionalizing the DPB.
Civil Damages	Explicit right for non-material harm.	Negligence-based statutory compensation.
Cross-Border	Strict adequacy/SCC requirements.	Negative-list approach (government notified).

3.15 Critical Evaluation

Doctrinally, current statutory frameworks exhibit several ambiguities that complicate corporate operations. First, neither the EU nor India treats personal data as "property" in the classical sense.[172] This avoidance of commodification prevents individuals from "selling" their privacy but complicates asset-based valuation models; value is derived from the *right to process* rather than *ownership of the data*.

Second, AI systems challenge traditional legal classifications. They are hybrid assets composed of copyrighted code, licensed datasets, and machine-generated weights. No single doctrinal category captures this complexity, requiring M&A diligence to dissect each component individually.

Third, while the "undertaking" concept in the EU ensures that corporate groups cannot evade liability through shell companies, it creates significant friction for group structuring and internal cost-allocation. Ultimately, modern data laws prioritize regulatory objectives over transactional convenience, forcing corporate law to adapt through increasingly layered diligence and contractual safeguards.

[1]Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism,* 1st ed. (Oxford University Press, 2019).
[2]Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* 1st ed. (PublicAffairs, 2019).
[3]Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism, 1st ed. (Oxford University Press, 2019).*
[4]Organisation for Economic Co-operation and Development, *OECD Privacy Framework* (OECD Publishing, 2013).
[5]Avtar Singh, *Company Law,* 17th ed. (Eastern Book Company, 2020).
[6]A.Ramaiya, *Guide to the Companies Act*, 18TH ed. (LexisNexis, 2019).
[7]Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,* 1st ed. (W.W. Norton, 2015).
[8]Digital Personal Data Protection Act, 2023.
[9]Regulation (EU) 2016/679 of the European Parliament and of the Council(General Data Protection Regulation).
[10]Christopher Kuner, _*The GDPR and the Challenge of International Data Transfers*' (2017) 2 International Data Privacy Law 1.
[11]Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information,* 1st ed. (Harvard University Press, 2015).
[12]Avtar Singh, *Company Law*, 17th ed. (Eastern Book Company, 2020).
[13]L. C. B. Gower and Paul L. Davies, *Principles of Modern Company Law*, 10th ed. (Sweet & Maxwell, 2016).
[14] A. Ramaiya, *Guide to the Companies Act*, 18th ed. (LexisNexis, 2019).
[15]Umakanth Varottil, _The Evolution of Corporate Law in Post-Colonial India: From Transplant to Autochthony' (2014) 31 *National Law School of India Review* 253
[16] Umakanth Varottil, _Corporate Governance in India: The Transition from Code to Statute' (2014) 7 *NUJS Law Review* 1.
[17]Somasekhar Sundaresan, *Securities Law in India* (LexisNexis, 2017).
[18] L. C. B. Gower, Paul L. Davies and Sarah Worthington, *Principles of Modern Company Law*, 10th ed. (Sweet & Maxwell, 2016).
[19]Daniel J. Solove, _Privacy as Regulation' (2006) 65 *Washington and Lee Law Review* 923.
[20]Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, 2019).
[21]Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, 2019).
[22]Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013). [23]Organisation for Economic Co-operation and Development, *OECD Privacy Framework* (OECD Publishing, 2013).
[24] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)*, 1981.
[25] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995.
[26] Information Technology Act, 2000.
[27] The Competition Act, 2002
[28] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[29]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[30] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016.
[31] Digital Personal Data Protection Act, 2023
[32]The Companies Act, 1956 (Act 1 of 1956).
[33]For an overview of the 1991 reforms, see Bimal Jalan, *India's Economic Reforms: A New Era* (1992).
[34]The Competition Act, 2002 (Act 12 of 2003).
[35] Information Technology Act, 2000 (Universal Law Publishing, New Delhi, 2000).
[36] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[37]*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1
[38] V.K. Ahuja, *Law Relating to Intellectual Property Rights* p. 452 (LexisNexis, Gurugram, 3rd edn., 2017)
[39] Copyright Act, 1957

[40]*Supra* note 4 at p. 458.
[41] Richard Whish and David Bailey, *Competition Law* p. 832 (Oxford University Press, Oxford, 10th edn., 2021).
[42] Council Regulation (EEC) No. 4064/89 of 21 December 1989 on the control of concentrations between undertakings.
[43] Whish and Bailey, *supra* note 1 at p. 850
[44] Council Regulation (EC) No. 139/2004 of 20 January 2004 on the control of concentrations between undertakings.
[45] European Convention on Human Rights, art. 8.
[46] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981 (ETS No. 108)
[47] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2018 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[49] Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases.
[50] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified Version).
[51] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
[52]Richard Whish and David Bailey, *Competition Law* p. 845 (Oxford University Press, Oxford, 10th edn., 2021).
[53]European Convention on Human Rights, art. 8.
[54]Convention 108 (1981).
[55]Julie E. Cohen, *Between Truth and Power* (OUP, 2019).
[56]Information Technology Act, 2000.
[57]*Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[58]Directive 95/46/EC.
[59]Information Technology Act, 2000
[60]SPDI Rules, 2011.
[61]*Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[62]Regulation (EU) 2016/679 (GDPR)
[63]Regulation (EC) No. 139/2004.
[64]Gower & Davies, *Principles of Modern Company Law* (Sweet & Maxwell, 2016).
[65]Competition Act, 2002
[66]Directive 96/9/EC (Database Directive).
[67]Copyright Act, 1957.
[68]V.K. Ahuja, *Law Relating to Intellectual Property Rights* p. 510 (LexisNexis, Gurugram, 3rd edn., 2017) [69]Richard Whish and David Bailey, *Competition Law* p. 865 (Oxford University Press, Oxford, 10th edn., 2021)
[70]*Supra* note 1 at p. 515
[71]*Ibid*
[72] Whish and Bailey, *supra* note 2 at p. 870
[73]*Ibid.*
[74]*Supra* note 1 at p. 522.
[75] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2018 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[76] Digital Personal Data Protection Act, 2023
[77]*Supra* note 1 at art. 25.
[78]*Supra* note 2 at s. 4
[79]*Supra* note 1 at art. 83.
[80]V.K. Ahuja, *Law Relating to Intellectual Property Rights* p. 510 (LexisNexis, Gurugram, 3rd edn., 2017).
[81]Ibid.
[82]Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases.
[83]*Supra* note 1 at p. 515.
[84]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2018 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

[85]Ibid.
[86]Digital Personal Data Protection Act, 2023.
[87]*Supra* note 5 at art. 4.
[88]*Supra* note 3.
[89]*Supra* note 1 at p. 458. [90]Copyright Act, 1957, s. 2(ffc) [91]*Supra* note 1 at p. 462.
[92]*Ibid.*
[93]*Supra* note 1 at p. 520.
[94]Digital Personal Data Protection Act, 2023, s. 8.
[95]*Ibid*, s. 3.
[96]*Ibid*, s. 8(5).
[97]*Ibid*
[98]Companies Act, 2013, s. 166.
[99]Digital Personal Data Protection Act, 2023, s. 8(6).
[100]*Ibid*, s. 6.
[101]*Ibid*.
[102]*Ibid*, s. 7.
[103]*Ibid.*, s. 10.
[104]*Ibid*. [105]*Ibid.*, s. 8(2).
[106]*Ibid.*, s. 33 read with Schedule.
[107]Information Technology Act, 2000 (Universal Law Publishing, New Delhi, 2000).
[108]*Ibid.*, s. 43A
[109]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[110]*Supra* note 1 at s. 43A.
[111]*Supra* note 3, r. 4-5.
[112]CERT-In, *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000* (issued on April 28, 2022).
[113]*Supra* note 1, s. 79.
[114]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[115]*Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[116]*Google India Pvt Ltd v. Visaka Industries*, (2020) 4 SCC 162.
[117]Companies Act, 2013, s. 166.
[118]SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.
[119]*Supra* note 11, s. 134.
[120]SEBI, *Business Responsibility and Sustainability Reporting (BRSR) Framework* (2021).
[121]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2018 on theprotection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[122]*Ibid.*, art. 5(2).
[123]*Ibid.*, art. 28.
[124]*Ibid.*, art. 26.
[125]Richard Whish and David Bailey, *Competition Law* p. 845 (Oxford University Press, Oxford, 10th edn.,2021).
[126]*Supra* note 1, art. 24.
[127]*Ibid.*, art. 30.
[128]*Ibid.*, art. 37-39.
[129]*Ibid.*, art. 35.
[130]EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (2020).
[131]*Supra* note 5 at p. 852
[132]*Supra* note 1, art. 83.
[133]*Ibid.*, art. 83(1).
[134]*Ibid.*, art. 58.
[135]*Supra* note 1, art. 5.
[136]*Ibid.*, art. 22.
[137]*Supra* note 10.
[138]*Supra* note 1, art. 13-14

[139]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
[140]Companies Act, 2013, s. 166.
[141]*Ibid.*, s. 134(3)(n).
[142]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2018 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), art. 83
[143]*Ibid.*, art. 5(2)
[144]*Ibid.*, art. 37.
[145]*Ibid.*, art. 38
[146]*Ibid.*, art. 39
[147]*Ibid.*, art. 38(3)
[148]Digital Personal Data Protection Act, 2023, s. 10(2)(a)
[149]Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 5(9).
[150]Companies Act, 2013, s. 134(5)(e)
[151]*Supra* note 3, art. 32.
[152]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2018 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[153]*Ibid.*, art. 5(2).
[154]*Ibid.*, art. 35.
[155]Digital Personal Data Protection Act, 2023. [156]Information Technology Act, 2000, s. 43A. [157]*Supra* note 1 at art. 37.
[158]*Ibid.*, art. 83.
[159]*Supra* note 1 at art. 5(1)(b).
[160]V.K. Ahuja, *Law Relating to Intellectual Property Rights* p. 520 (LexisNexis, Gurugram, 3rd edn., 2017).
[161]*Ibid.* at p. 525.
[162]*Supra* note 1 at art. 6.
[163]Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases
[164]Regulation (EU) 2016/679 (General Data Protection Regulation), art. 83(5).
[165]*Deutsche Wohnen SE v. Staatsanwaltschaft Berlin*, Case C-807/21 (2023).
[166]Digital Personal Data Protection Act, 2023, s. 33 r/w Schedule.
[167]Information Technology Act, 2000, s. 43A
[168]*Supra* note 1 at art. 82
[169]*UI v. Österreichische Post AG*, Case C-300/21 (2023)
[170]*Supra* note 4.
[171]SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015.
[172]V.K. Ahuja, *Law Relating to Intellectual Property Rights* p. 525 (LexisNexis, Gurugram, 3rd edn., 2017).