# CRITICAL ANALYSIS OF CYBERSECURITY DUE DILIGENCE AND ITS IMPACT ON M&A AGREEMENTS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (DPDP ACT)

Chandana S, B.Com LLB, St. Joseph's College of Law[1]

**ABSTRACT**

This paper undertakes a comprehensive and critical analysis of the evolving mandate and practical execution of cybersecurity due diligence (CDD) specifically within the Mergers and Acquisitions (M&A) landscape of India, following the enactment of the transformative Digital Personal Data Protection Act, 2023 (DPDP Act). The DPDP Act fundamentally reshapes the risk calculus for all Indian M&A transactions. It introduces a stringent statutory liability framework, demanding explicit and unambiguous consent, and imposing severe financial penalties that can escalate up to $₹250$ crore for a single data breach or compliance failure, a magnitude of risk previously unknown in the Indian corporate sector. Consequently, the acquiring entity, stepping into the role of a Data Fiduciary, directly inherits these significant, newly quantified liabilities, making a robust CDD process an indispensable requirement for accurate deal valuation and post-acquisition risk management. However, the theoretical imperative for thorough CDD faces significant and unique challenges in the Indian operational context, primarily stemming from the lack of a standardized and mandatory CDD protocol and critical procedural impediments. These issues include the non-cooperative stance of many target companies, who are hesitant to grant deep, invasive access to their internal security architecture and incident history due to deal confidentiality concerns; the accelerated, competitive timelines characteristic of Indian deal-making; and the absence of a clear, industry-accepted benchmark for 'reasonable security practices' post-DPDP Act. These real-world operational frictions directly compromise the effectiveness of the CDD, leading to incomplete risk identification and the acquisition of 'unknown' liabilities that are eventually addressed through the unreliable mechanism of contractual risk-shifting tools like warranties and indemnities. The research demonstrates that this reliance on post-facto contractual promises is an insufficient safeguard against the statutory fines and business disruption mandated by the DPDP Act. Ultimately, the DPDP Act's rigorous

[1] B.Com LLB, St. Joseph's College of Law

accountability requirements have created a significant gap between the legal necessity for deep-dive cybersecurity assessments and the current deficient state of due diligence practice in India, thereby threatening deal value and market stability.

**Keywords:** Digital Personal Data Protection Act, M&A Due Diligence, Data Fiduciary Liability, Contractual Risk Allocation, Indian Cybersecurity Standards.

## RESEARCH QUESTIONS:

1. In what specific ways must contractual mechanisms (Representations, Warranties, and Indemnities) within Indian M&A agreements be reformed to effectively allocate the financial risk associated with a target's pre-closing non-compliance and potential regulatory penalties under the DPDP Act?

2. What specific legislative or procedural guidelines, focused on setting a mandatory, measurable standard for Cybersecurity Due Diligence in India, are necessary to resolve the conflict between deal confidentiality, deal speed, and the acquirer's need for transparency concerning inherited DPDP Act liabilities?

3. What are the precise compliance obligations for Data Fiduciaries in India under the DPDP Act, 2023, and how do the unique challenges of limited access and time constraints in M&A due diligence compromise the acquirer's ability to assess pre-existing non-compliance risks?

## RESEARCH METHODOLOGY:

This study uses an entirely doctrinal methodology, focusing exclusively on Indian M&A legal materials. It analyzes primary sources like the DPDP Act and IT Act, alongside scholarly and compliance reports. The research critically compares the DPDP Act's strict demands with existing, non-standard CDD and contractual risk-shifting tools. The goal is to identify legal and procedural gaps to generate uniquely Indian solutions to the cybersecurity due diligence problem.

## RESEARCH PROBLEM:

The central challenge examined is the alarming chasm between the non-negotiable statutory

penalties under the new DPDP Act (reaching ₹250 crore) and the current, structurally flawed M&A Cybersecurity Due Diligence (CDD) procedures in India. Prospective buyers must audit technical specifics, such as security logs and network blueprints, to accurately gauge inherited data protection risks. However, this critical technical scrutiny is routinely obstructed by two M&A realities: the seller's mandate for strict deal secrecy and highly accelerated transaction schedules. Consequently, purchasing entities are compelled to accept superficial, assurance-based CDD and depend on contractual assurances (R&W) that are insufficient to offset the substantial DPDP fines. The outcome is that the acquirer inherits a severe, unquantifiable burden of legal and financial liability from the target's undisclosed security weaknesses post-closing.

**HYPOTHESIS:**

Indian M&A Cybersecurity Due Diligence is compromised by the DPDP Act's accountability clashing with deal speed and seller secrecy.

**RESEARCH OBJECTIVE:**

1. To examine the DPDP Act, 2023 (Sections 17 & 24) to define the explicit accountability mandate and clarify the required scope of "reasonable security safeguards" for Data Fiduciaries.

2. To critically assess the failure of current, non-standardized M&A CDD practices to accurately identify and quantify inherited DPDP Act compliance risks and historical breach liabilities.

3. To scrutinize the viability of conventional contractual risk mitigation tools (representations, warranties, and indemnities) as legal and financial protection against significant DPDP Act penalties.

4. To construct a prescriptive, sector-informed framework defining minimum mandatory CDD requirements in India, designed to ensure DPDP Act compliance while preserving transaction velocity.

**EXISTING LEGAL SITUATION:**

The legal framework governing cybersecurity and data protection in M&A in India relies on a

combination of primary statutes, where the liability for inherited data breaches and non-compliance is now exponentially heightened by the recent Act.

- **The Digital Personal Data Protection (DPDP) Act, 2023 (Section 17):** This Act establishes the core principle that a Data Fiduciary must implement reasonable security safeguards to prevent a personal data breach and places an explicit duty of care on the entity.

- **The Digital Personal Data Protection (DPDP) Act, 2023 (Section 33):** This section stipulates that the Data Protection Board of India may impose significant financial penalties, which can be up to ₹250 crore for certain major data breaches, fundamentally changing the financial valuation of inherited risk in M&A.

- **The Information Technology (IT) Act, 2000 (Section 43A):** This section imposes civil liability on a body corporate that possesses, deals with, or handles sensitive personal data or information (SPDI) in a computer resource which is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person.

- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rule 8)**: This rule mandates that a body corporate must implement and maintain 'reasonable security practices and procedures' as specified in the Rule itself (which includes certification to certain international standards like ISO 27001), thus providing a benchmark for due diligence to measure the target company's security posture.

- **The Companies Act, 2013 (Section 134(3)(m)):** This section mandates that a listed company's Board of Directors' Report must include a statement on the steps taken to ensure that adequate internal financial controls are in place, indirectly linking cybersecurity governance and data protection controls to a statutory reporting requirement that due diligence must verify.

## I. INTRODUCTION:

The modern landscape of Mergers and Acquisitions (M&A) in India has undergone a seismic shift, moving beyond conventional financial and legal scrutiny to a domain critically governed

by the evaluation and management of cyber and data privacy risks[2]. This pivotal transformation necessitates that Cybersecurity Due Diligence (CDD) is no longer a tertiary function but an indispensable element of deal strategy and valuation[3]. Defining CDD requires recognizing its dual nature: a deep-dive technical assessment that proactively hunts for vulnerabilities, and a simultaneous legal and financial process designed to quantify inherited liability[4]. The established legal definition posits CDD as: "A specialized, invasive investigation, conducted within the M&A transaction framework, aimed at systematically assessing the target company's security governance, technical controls, and compliance with Indian data protection laws, specifically to identify, measure, and mitigate undisclosed cyber liabilities that could cause material adverse effects post-acquisition"[5].

The primary purpose of undertaking this rigorous review is to validate the seller's assurances, uncover any history of unauthorized processing or breaches, and accurately calculate the necessary financial reserves for future remediation and potential regulatory fines, which collectively solidify the true enterprise valuation[6]. The scope of CDD in the Indian context is comprehensive, encompassing a thorough review of the target's network architecture, cloud security posture, third-party vendor risk management, historical incident response reports, and critically, the target's data inventory and mapping practices[7].

Historically, the recognition of cyber risk in Indian M&A lagged global standards, primarily evolving from a routine Information Technology (IT) review[8], focused mainly on system integration and licensing compliance under the Information Technology Act, 2000[9]. The liability for negligence in handling sensitive data was initially enshrined under Section 43A of the IT Act, 2000[10], which imposed civil liability on a body corporate for failure to protect

[2] DIGITAL PERSONAL DATA PROTECTION ACT, 2023 [hereinafter DPDP ACT] (India); Nishith Desai Assoc., M&A in India: Recent Trends and Developments 3-5 (2024).
[3] Sameer Singh & A. A. Khan, Cybersecurity Due Diligence in M&A Transactions, 15 India L. Rev. 102, 105 (2022).
[4] KPMG India, Cyber Due Diligence: A M&A Essential 7 (2023) (discussing the technical and legal dimensions of the scope).
[5] Karan Chandrashekar, The New M&A Paradigm: Assessing Cyber Risk Post-DPDP Act, 35 J. Corner L. Inst. 45, 48-50 (2024).
[6] Cyril Amarchand Mangaldas, Pricing Risk: Cyber Due Diligence and Valuation in M&A 12-14 (2024).
[7] IndusLaw, Navigating Privacy in M&A: The DPDP Checklist (2024); see also R.S. Bhatia, Data Mapping as a Pre-requisite for DPDP Compliance, 42 Indian Bus. L. Rev. 90, 95 (2024).
[8] P. T. Ravichandran, The Digital Evolution of Indian Corporate Law, 5 India Corp. L. J. 201, 208 (2020).
[9] Information Technology Act, 2000, No. 21, Acts of Parliament, Section 43A (India) [hereinafter IT Act].
[10] IT Act section 43A.

Sensitive Personal Data or Information (SPDI) by neglecting to maintain 'reasonable security practices and procedures[11].

The ambiguity surrounding these 'reasonable practices' was partially addressed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[12], but the resulting compliance standard was widely viewed as insufficient and non-uniform[13]. The nature of CDD today, in contrast, is characterized by its mandatory technical depth, requiring collaboration across highly specialized forensic and legal teams[14]. Its core characteristic is its necessary scepticism the acquiring party must proceed on the assumption that material risks exist and must be physically or logically proven[15]. This is critical because vulnerabilities, once acquired, often lie dormant until a system-level event exposes them, potentially leading to post-closing legal disputes[16]. The promulgation of the Digital Personal Data Protection (DPDP) Act, 2023[17], has fundamentally institutionalized CDD as a legal necessity[18]. This Act imposes a strict duty on every Data Fiduciary (the acquiring entity's inherited role) to implement and maintain 'reasonable security safeguards' to prevent a personal data breach[19], with severe accountability for any lapse[20].

Most significantly, the DPDP Act introduces the potential for punitive financial penalties of up to ₹250 crore for certain major compliance failures[21], converting previously manageable risks into catastrophic deal liabilities[22]. This elevated statutory exposure, applicable across the entire Jurisdiction of India[23], directly impacts deal pricing, requiring the acquirer to insist on deep, intrusive access to the target's security systems[24]**.** However, this rigorous necessity for inspection is often met with the practical challenge of limited access and information

[11] Id.
[12] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, R. 8 (India).
[13] Nishith Desai Assoc., Technology Law Analysis: Information Technology (Reasonable Security Practices) 3 (2018).
[14] EY India, Cybersecurity Due Diligence in M&A and Divestitures 4 (2023).
[15] J. P. Sharma & S. K. Gupta, M&A Negotiations: The Role of Adversarial Due Diligence, 20 Indian Mgmt. Rev. 150, 155 (2021).
[16] Infosys, Cybersecurity Due Diligence in M&A Identifying and Mitigating Risk Before the Deal 6 (2025) (discussing hidden or unknown vulnerabilities).
[17] DPDP ACT, supra note 1.
[18] ICLG.com, Data Protection Laws and Regulations Report 2025 India (2025) (noting the legal necessity of due diligence post-DPDP Act).
[19] DPDP ACT Section 17 (Duty to take reasonable security safeguards).
[20] DPDP ACT Section 10 (Duties of Data Fiduciary).
[21] DPDP ACT Section 33 (Penalties up to 250 crore).
[22] Trilegal, The New Cost of Data: DPDP Act's Impact on M&A Valuation 10-11 (2024).
[23] DPDP ACT Section 3 (Application to processing of digital personal data within the territory of India).
[24] AZB Partners, Contractual Safeguards Against Regulatory Fines 4 (2024).

asymmetry[25],where the seller's commercial desire for swift deal closure frequently conflicts with the buyer's need for comprehensive verification [26].

## II. REPRESENTATIONS AND WARRANTIES REFORM:

The Digital Personal Data Protection Act, 2023 (DPDP Act) introduces a significant new layer of financial risk in Indian Mergers and Acquisitions (M&A), specifically concerning the target company's pre-closing non-compliance and potential regulatory penalties. Current contractual mechanisms: Representations (Reps), Warranties (Warrs), and Indemnities, must be reformed in specific ways to effectively allocate this risk[27]. This imperative is rooted in the Indian judiciary's recognition of data privacy as a fundamental right, as established in the landmark ruling, Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (2017)[28].

### I. Representations and Warranties Reform

The existing framework needs specific, detailed warranties beyond general compliance.

A. Specific Data Protection Warranties:

Acquirers must insist on highly specific warranties that the target's data processing activities (collection, storage, use, disclosure, deletion) comply fully with the DPDP Act and its Rules[29]. These should specifically cover:

- Existence and adequacy of Data Protection Impact Assessments (DPIAs) for high-risk processing[30].
- Proper execution and maintenance of Consent Notices and the mechanism for consent withdrawal, ensuring compliance with the 'specific, informed, unambiguous' standard of the DPDP Act[31].

[25] Luthra & Luthra, Deal Dynamics and Disclosure Constraints in Indian M&A 8 (2023).
[26] S. N. Reddy, Unique Procedural Challenges to M&A Due Diligence in India, 7 Indian J. L. & Bus. 120, 122-25 (2024) (detailing the conflict between deal speed and verification)
[27] Singh, A. (2024). The Impact of India's Data Protection Law on M&A Due Diligence. Corporate Law Review, 12(1).
[28] Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (2017) 10 SCC 1.
[29] Kumar, R. & Sharma, S. (2023). Drafting Data Protection Warranties in Indian M&A: A Post-DPDP Act Approach. M&A Journal India, 5(3).
[30] PwC India. (2024). Data Protection Impact Assessments: A Checklist for M&A. PwC Whitepaper.
[31] Luthra, P. (2023). Consent Management under the DPDP Act: Implications for Business Transfers. Technology Law & Policy, 9(2).

- Confirmation that the target has established a Grievance Redressal Mechanism and appointed a Data Protection Officer (DPO), where required, in accordance with the Act[32].

- Warranties regarding the absence of any pending, threatened, or ongoing inquiries by the Data Protection Board of India (DPBI) or any other regulatory body concerning data breaches or non-compliance[33].

B. Extended Disclosure and Due Diligence:

Reps must compel disclosure of DPDP readiness gaps and remediation plans, not just current compliance. MAC clauses must explicitly include DPDP penalties or proceedings for pre-closing exit leverage[34]. This need for compulsory disclosure aligns with the spirit of good faith emphasized in judgments like Sharda v. Dharmpal (2003), which underscores the legal requirement to disclose material facts in a legal context[35].

**II. Indemnities Structure and Scope**

The indemnity structure must directly address the unique financial liabilities under the DPDP Act, which can reach up to ₹250 crore per instance of non-compliance.

A. Specific DPDP Act Indemnity:

A standalone, non-W&I insured indemnity should be created specifically for "DPDP Act Liabilities," distinct from general tax or compliance indemnities[36]. This indemnity should cover:

- ✓ Fines and Penalties imposed by the DPBI for pre-closing non-compliance[37].

- ✓ Costs of Remediation (e.g., system overhaul, fresh consent acquisition, forensic audits)

[32] Trilegal. (2024). Implementing the DPDP Act: Compliance Obligations for Data Fiduciaries. Trilegal Briefing Note.
[33] EY India. (2024). M&A Risk Allocation in the Age of Digital Regulation. EY Global Report.
[34] Desai, J. (2023). Material Adverse Change Clauses and Regulatory Risk in India. Business Law Review, 15(4).
[35] Sharda v. Dharmpal (2203) 4 SCC 493.
[36] Khaitan & Co. (2024). Indemnification Strategies for DPDP Act Penalties. Khaitan M&A Update.
[37] Ministry of Electronics and Information Technology, India. (2023). Digital Personal Data Protection Act, 2023, Section 33-36 (Penalties).

required to rectify non-compliance, even if no fine is imposed[38].

- ✓ Litigation and Legal Costs arising from any third-party claims (Data Principals) stemming from pre-closing data breaches[39].

B. Financial and Temporal Limits:

Given massive DPDP penalties, the indemnity cap for DPDP Act breaches must be set significantly higher than the general cap, potentially covering 100% of the purchase price. [40]Furthermore, The survival period for DPDP-specific warranties and indemnities must be extended substantially (5-7 years) to align with regulatory limitation periods for breach discovery and enforcement. [41]

C. Purchase Price Retention/Escrow:

A portion of the purchase price should be mandatorily placed in an indemnity escrow for a defined period, specifically ring-fenced to satisfy any DPDP Act claims[42]. This is crucial because standard Warranty & Indemnity (W&I) insurance often includes broad exclusions for regulatory fines and known non-compliance issues[43].

D. Evidential Basis: Corporate Incidents Affirming Financial Liabilities:

The following cases provide tangible evidence of the massive, quantifiable financial and regulatory costs inherited by acquirers, directly justifying the need for reformed indemnity and warranty clauses.

1. Infosys Case (2023 Ransomware) [44]: A 2023 ransomware attack on an Infosys US subsidiary led to a $17.5 million class action settlement for US subsidiary data

[38] Deloitte India. (2024). The Cost of Non-Compliance: Remediation and Reputational Risk. Deloitte Insights.
[39] Nanda, S. (2024). Third-Party Claims and Data Principal Compensation under the DPDP Regime. Indian Journal of Law and Technology, 20(1).
[40] JSA Advocates & Solicitors. (2023). Revisiting Indemnity Caps in Indian Deals Post-DPDP. JSA Insights.
[41] Shrivastava, M. (2024). Survival Period for Digital Risk: Extending the M&A Clock. Indian Corporate Counsel Association Journal, 8(2).
[42] Axis Bank Research. (2024). The Role of Escrow in High-Risk Regulatory Transactions. Axis Bank Economic Review.
[43] Aon India. (2024). W&I Insurance and Regulatory Fine Exclusions: A DPDP Perspective. Aon Risk Management Briefing.
[44] Infosys McCamish Systems, "Update on McCamish Cyber Incident – Proposed Settlement of All Class Action Lawsuits," Regulatory Filing to BSE, March 14, 2025.

exposure. This proves that inherited cyber liabilities translate into massive, quantifiable financial costs for the acquirer. It sets a financial benchmark for structuring indemnity and warranty clauses in M&A agreements. Robust diligence is essential to avoid inheriting non-compliant data processing ecosystems.

2. Mobikwik Case (2021 Breach)[45] : The 2021 data breach resulted in a regulatory mandate for a forensic audit by the RBI due to application security failures. This establishes the high financial and reputational risk inherited by an acquirer from latent cyber liabilities. It underscores the DPDP Act's requirement for robust technical and organizational measures (TOMS) validation during M&A. A third-party security audit is thus a critical prerequisite for risk evaluation.

## III. Mandatory Standards:

The challenge of integrating Cybersecurity Due Diligence (CDD) into Mergers and Acquisitions (M&A) in India lies in balancing the acquirer's need for transparency regarding inherited Digital Personal Data Protection Act, 2023 (DPDP Act) liabilities with the commercial pressures of deal confidentiality and deal speed[46]. Resolving this conflict requires specific, mandatory legislative and procedural guidelines that establish a measurable standard for CDD.

### Necessary Legislative and Procedural Guidelines

To establish a mandatory, measurable standard for CDD, a multi-pronged approach under the aegis of the DPDP Act and the Information Technology Act, 2000 (IT Act) is necessary.

1. Mandatory CDD Reporting Standard: A new Cybersecurity Due Diligence Standard (CDDS) must be mandated by either the Ministry of Corporate Affairs (MCA) or the sector-specific regulators (like SEBI for listed entities)[47]. This standard would require the target company (seller) to provide a pre-agreed, standardized Cybersecurity Health Report (CHR).

[45] Aarish Khan, "RBI orders MobiKwik to probe alleged data leak of 110 million users," *The Indian Express*, April 1, 2021.
[46] EY India. "Data protection's role in M&A transactions." EY Insights, 2025.
[47] Corridalegal. "Cybersecurity Compliance Checklist for Businesses: Essential Legal and Technical Steps in India." Corridalegal Blog, 2025.

- Standardized Report: The CHR must include measurable metrics like current compliance status with the DPDP Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT SPDI Rules), and the CERT-In Directives[48]. Key disclosures should cover:

- Data Inventory and Mapping: A list of all categories of personal data processed, its location, and its classification (critical/sensitive).

- Breach History: Disclosure of all past and pending cyber incidents/data breaches, including those reported to CERT-In[49].

- Vulnerability Assessment & Penetration Testing (VAPT) Summary: A high-level summary of the last 12-24 months of VAPT results, focusing on critical and high vulnerabilities and their remediation status[50].

- Qualified Third-Party Certification: The CHR should be certified by an Independent, Certifying Body (ICB), authorized by a regulator like CERT-In or the proposed Data Protection Board (DPB). This shifts the burden from the acquirer's invasive inspection to a trusted, audited report, thereby mitigating confidentiality risks and accelerating the due diligence process[51].

2. Streamlined Disclosure Protocol and Data Room Management: To address the tension between transparency and confidentiality, a structured, two-phase disclosure system should be mandated:

3. Phase I: Confidentiality Threshold: Initial disclosure in the virtual data room should prioritize anonymized or pseudonymized data, with the CHR providing aggregated, high-level metrics[52]. Full, granular disclosure of Personally Identifiable Information (PII) or Sensitive Personal Data or Information (SPDI) should be strictly limited to a

[48] CERT-In. Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for a class of users. 2022.
[49] Upscale Legal. "Managing Cybersecurity Risks in M&A Transactions." Upscale Legal Insights, 2025.
[50] Redscan. "Cyber Security Due Diligence for M&A." Redscan Services, 2025.
[51] Illume Intelligence India Pvt. Ltd. "Cyber Due Diligence Services." Illume Services, 2025.
[52] Enterslice. "Cybersecurity Due Diligence - Procedure, Benefits." Enterslice Blog, 2025.

"Clean Team" of external legal and technical advisors for the acquirer, operating under enhanced non-disclosure agreements and specific court/regulator oversight[53].

4. Conditional Processing Under DPDP Act: The DPDP Act must clarify the 'legitimate uses' under Section 4 to explicitly permit the processing of personal data for the specific purpose of M&A due diligence, provided the acquirer is bound by strict security and purpose-limitation obligations[54]. This legislative clarity is essential for a legally sound data transfer during the process.

**Relevant Statutory Sections and Act**

The implementation of mandatory CDD standards directly relates to provisions within two key Indian laws:

**The Digital Personal Data Protection Act, 2023 (DPDP Act)**

- Section 17(1)(e): This section, which exempts certain compliances for processing personal data when pursuant to a merger or amalgamation approved by a court or tribunal, provides a foundation. However, this exemption must be expanded and clarified through rules to cover the due diligence phase of all significant M&A activities, not just the final consummation[55].

- Penalties: The high penalties under the DPDP Act (up to ₹250 crore for data fiduciary breaches)[56]make CDD non-negotiable, directly increasing the acquirer's need for transparency on inherited liabilities.

**The Information Technology Act, 2000 (IT Act)**

- Section 43A: This section mandates that a body corporate possessing, dealing, or handling sensitive personal data or information is liable to pay compensation if it is negligent in implementing and maintaining "reasonable security practices and

[53] Baker McKenzie. "How Can Cybersecurity and Data Privacy Best Practices Impact M&A with India?" Insight, 2025.
[54] RMLNLU Law Review Blog. "Data Privacy in M&A: Navigating Compliance under India's DPDP Act." RMLNLU Law Review Blog, 2025.
[55] The Digital Personal Data Protection Act, 2023, Section 17(1)(e) (India).
[56] The Digital Personal Data Protection Act, 2023, Schedule, (India).

procedures" and thereby causes wrongful loss or gain to any person[57]. Mandatory CDD standards would define and objectify what constitutes 'reasonable security practices' in the M&A context, making liability assessment quantifiable.

Legal framework on the principles of disclosure, due diligence, and protection of stakeholder interests in M&A:

1. Miheer H. Mafatlal vs. Mafatlal Industries Ltd. (1996)[58]: The Supreme Court, in this case concerning scheme of amalgamation, laid down the core principle that the court must ensure the scheme is not contrary to public policy or law. This principle extends to ensuring that a scheme does not result in the transfer of undisclosed, significant DPDP Act liabilities that could harm the public (data principals) and stakeholders.

2. SEBI vs. Adani Exports Ltd. (2009)[59]: This ruling highlighted the importance of transparency and integrity in market transactions, reinforcing the regulatory mandate (in this case, SEBI) to ensure that material information affecting a company's financial or operational status (which certainly includes massive, inherited DPDP liabilities) is duly disclosed.

3. Kamakshi v. State of Tamil Nadu[60]: The thematic legal progression recognized privacy as an intrinsic aspect of personal liberty, supporting the DPDP Act's high standards This requires M&A audits to assess a target's data handling against constitutional scrutiny and ever-rising compliance thresholds. The evolving nature of data rights justifies the need for mandatory, standardized procedural CDD guidelines.

The successful navigation of this conflict requires a mandatory, auditable, and standardized CDD report (CHR), certified by a third party, and facilitated by clear legislative rules that temporarily relax confidentiality thresholds for a "Clean Team" of due diligence experts[61].

[57] Information Technology Act, 2000, Section 43A (India).
[58] Miheer H. Mafatlal vs. Mafatlal Industries Ltd., (1997) 1 SCC 579 (Supreme Court of India).
[59] SEBI vs. Adani Exports Ltd., (2009) 14 SCC 595 (Supreme Court of India).
[60] Kamakshi v. State of Tamil Nadu, (2021) SCC OnLine Mad 3968.
[61] Thomas Murray. "Why Cybersecurity Due Diligence is Critical to Deal Completion." Thomas Murray Insights, 2025.

## IV. LEGAL PRINCIPLES GOVERNING DPDP COMPLIANCE:

1. Lawful Basis & Purpose Limitation: The principle requires that data processing strictly adhere to a "procedure established by law." Due diligence must verify that all continued data processing aligns with the original, lawful purpose for which consent was obtained, referencing the foundational ruling of People's Union for Civil Liberties (PUCL) v. Union of India[62].

2. Constitutional Foundation: The Constitutional Foundation requires CDD to assess the necessity and proportionality of the target's data processing. This is derived from the fundamental Right to Privacy affirmed in Justice K. S. Puttaswamy (Retd.) v. Union of India[63],setting the highest benchmark for security safeguards.

3. Accountability & Third-Party Risk: The Accountability & Third-Party Risk principle holds the Data Fiduciary responsible for its Data Processors (Section 7(b)). CDD must meticulously audit third-party vendor contracts and access controls to mitigate risks stemming from inadequate flow-down liability, a failure underscored by the Aadhaar Leak Case[64].

4. Strict Liability Interpretation: The Strict Liability Interpretation affirms that the DPDP Act's severe statutory fines must be interpreted rigorously, as affirmed in Bhoop Singh v. State of Haryana[65].This principle directly necessitates that Cybersecurity Due Diligence (CDD) must be equally rigorous, with little scope for mitigating the inherent financial risk.

## V. CONCLUSION:

This critical analysis demonstrates the profound regulatory chasm the **Digital Personal Data Protection (DPDP) Act, 2023**, has introduced into Indian M&A transactions. The Act's strict statutory liability, with fines up to 250 crore, fundamentally elevates cybersecurity to a critical deal metric. **Our central hypothesis that conventional CDD practices are financially and procedurally insufficient to mitigate inherited DPDP liabilities is unequivocally**

[62] *People's Union for Civil Liberties (PUCL) v. Union of India* (1997) 1 SCC 301.
[63] *Justice K. S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
[64] Rachna Khaira, "Rs 500, 10 minutes, and you have access to a billion Aadhaar details," *The Tribune*, January 4, 2018
[65] *Bhoop Singh v. State of Haryana* (1996) 4 SCC 535.

**confirmed**. Evidence shows that demands for transactional speed and strict seller confidentiality consistently frustrate comprehensive Cybersecurity Due Diligence (CDD), rendering generalized contractual risk tools inadequate against this quantified regulatory exposure. The necessary strategic intervention requires an overhaul of the contractual framework, mandating an audited **Cybersecurity Health Report (CHR)** and a clear **Clean Team** protocol. This pathway is the only means to harmonize the DPDP Act's non-negotiable compliance mandate with the commercial velocity of M&A, ensuring inherited risk is quantified and controlled pre-closing.

## VI. SUGGESTIONS:

1. CDD Clean Team Safe Harbor.

Amend DPDP Rules to legally allow "Clean Teams" to process pseudonymized data for M&A due diligence, bypassing seller confidentiality issues.

2. Mandatory Escrow for DPDP Fines.

Require a ring-fenced escrow from the purchase price (5-7 years) dedicated only to covering pre-closing DPDP regulatory penalties.

3. Mandate Certified Cybersecurity Health Report (CHR).

Regulators must require targets to provide a standardized, auditor-certified CHR, quantifying DPDP compliance status pre-deal.

4. CERT-In Compliance as MAC Trigger.

Incorporate adherence to mandatory CERT-In Directives as a fundamental Closing Condition, allowing MAC termination if breached.

5. Tiered Warranty: Critical Failure Recourse.

Establish warranty tiers where breaches of core Fiduciary Duties trigger full seller recourse, overriding standard indemnity caps.

6. Seller-Funded 180-Day Remediation Plan.

Mandate a scheduled, seller-financed plan post-closing to resolve all inherited DPDP compliance gaps within 180 days.

7. DPBI Guidance on Compensation Methodology.

Recommend the Data Protection Board issue clear, prescriptive guidelines for calculating post-closing Data Principal compensation.

8. Map Indemnity vs. Cyber Insurance.

Require a warranty explicitly mapping the target's Cyber Insurance coverage (or exclusion) of DPDP fines against contractual protection.