CORPORATE CRIMINAL LIABILITY FOR DATA BREACHES UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL ANALYSIS

Aisha Tanvir, United University (LLM in Criminal and Forensic Law)

ABSTRACT

The exponential growth of the digital economy has transformed personal data into a valuable corporate asset, making organizations increasingly vulnerable to data breaches that threaten individual privacy, financial security, and public trust. In India, the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* prompted the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), which establishes a comprehensive legal framework for regulating the collection, processing, and protection of personal data. While the Act imposes extensive obligations on Data Fiduciaries and prescribes substantial monetary penalties for non-compliance, it does not expressly recognize corporate criminal liability for data breaches. This raises a significant legal question as to whether a predominantly regulatory and civil penalty regime is sufficient to ensure corporate accountability in cases involving serious negligence, reckless data management, or intentional misuse of personal data.

This paper critically examines the concept of corporate criminal liability in the context of data breaches under the DPDP Act, 2023. It analyses the statutory framework alongside the Information Technology Act, 2000 to evaluate the extent to which the existing legal regime addresses corporate misconduct involving personal data. Adopting a doctrinal research methodology, the study relies on statutory provisions, judicial precedents, government reports, and scholarly literature to assess the adequacy of the current framework. The paper argues that although the DPDP Act marks a significant advancement in India's data protection landscape by introducing stronger compliance obligations and enforcement mechanisms, its reliance on administrative penalties leaves important gaps in addressing grave corporate misconduct. It concludes that a more coherent legal framework, supported by effective enforcement, clearer standards of corporate accountability, and appropriate liability mechanisms, is essential to strengthen data governance and protect the constitutional right to informational privacy in India's rapidly evolving digital ecosystem.

Keywords: Corporate Criminal Liability; Data Breaches; Digital Personal Data Protection Act, 2023; Right to Privacy; Information Technology Act, 2000

Introduction

The concept of the Right to Privacy was first introduced in an essay by Samuel Warren and Louis Brandeis titled "The Right to Privacy," which was published in the Harvard Law Review in 1890. They argued that the "right to be left alone" should be recognized as an individual right and that existing laws should protect it as part of the human rights discussion. For corporate crimes, the legal maxim "Actus Non Facit Reum Nisi Mens Sit Rea" states that the accuser's intent and deeds must demonstrate culpability. Due to its numerous limitations, this rule is insufficient on its own. First, what is prohibited by law must be demonstrated in a court of law. As a result, even if the right to privacy has been recognized, it is still difficult to define. Privacy acknowledges the security of personal data as an essential component of human rights. right. The right to privacy through data protection is not only important but also an essential part of individual freedom and respect.

Achieving freedom in all spheres political, spiritual, religious, and even sexual is heavily impacted by data privacy. Numerous legal statutes, including those found in the Bhartiya Nyaya Sahinta, 2023 (Indian Penal Code) and the Information Technology Act of 2000, may fall under this responsibility. Basically, even if the Organizations may still be held accountable even if those directly responsible for data abuse are not found guilty.

Corporate criminal responsibility for data misuse means that a company may be charged with a crime if its workers or agents acting on its behalf use, disclose, or steal data illegally. This obligation is frequently limited to actions taken while working for the organization. When employees or agents of a company commit a crime while doing their duties and, to some part, for the benefit of the firm, corporate criminal culpability results.

Modern corporate landscapes are increasingly defined by digital technologies that facilitate the vast collection and analysis of personal information. Across industries including finance, aviation, e-commerce, healthcare, and digital services companies rely on data-driven models to streamline operations and boost consumer engagement. In this context, personal data has become a strategic asset, essential for commercial decision-making and maintaining a competitive edge.[1]

[1] Viktor Mayer-Schönberger & Thomas Ramge, *Reinventing Capitalism in the Age of Big Data* 12–15 (Basic Books, 2018).

However, this escalating reliance on digital infrastructure has heightened exposure to cybersecurity risks. Corporate data breaches stemming from unauthorized access, accidental disclosures, system failures, and malicious cyberattacks have become a frequent reality of the digital economy.[2]

Such incidents yield multidimensional consequences, ranging from economic loss and regulatory penalties to reputational damage and the long-term erosion of consumer trust. More significantly, data breaches directly undermine an individual's control over their personal information, raising grave concerns regarding privacy and human dignity.[3]

In India, frequent data breaches at private corporations have exposed systemic weaknesses in corporate data governance. Before the enactment of the DPDP Act, corporate liability for such breaches was managed through a fragmented framework under the Information Technology Act, 2000. These provisions were largely compensatory, lacked rigorous enforcement mechanisms, and failed to account for the scale and complexity of modern data processing.

The Supreme Court's landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India, fundamentally reshaped the legal landscape by establishing privacy as a constitutionally protected fundamental right under Article 21.[4] The Court clearly identified that informational privacy is jeopardized not only by state actions but also by private entities managing personal data.[5] Consequently, this constitutional mandate placed a duty on the State to enact a comprehensive legal framework to govern corporate data practices.

The Digital Personal Data Protection Act, 2023, serves as the legislative answer to this mandate. By instituting fiduciary responsibilities, compulsory security measures, breach notification protocols, and significant financial penalties, the Act aims to strike a new balance between fostering corporate innovation and safeguarding individual rights. The imposition of penalties reaching up to ₹250 crore marks a decisive transition from symbolic oversight to deterrence-focused enforcement. This paper explores the extent of corporate liability for data breaches under the Digital Personal Data Protection (DPDP) Act, 2023. It investigates whether

[2] World Economic Forum, *Global Cybersecurity Outlook 2024* (World Economic Forum, 2024).
[3] Computer Emergency Response Team-India (CERT-In), *Annual Report 2022–23* (Ministry of Electronics and Information Technology, Government of India, 2023), available at: https://www.cert-in.org.in, last visited on July 30, 2026.
[4] J*ustice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶¶ 242–247.

the current statutory framework effectively targets the structural origins of corporate data breaches and assesses its ability to enforce genuine accountability within India's fast-growing digital economy.

Research Questions

1. What is the concept and legal basis of corporate criminal liability in Indian jurisprudence?

2. What obligations does the Digital Personal Data Protection Act, 2023 impose on corporate entities (Data Fiduciaries) regarding the protection of personal data?

3. Does the Digital Personal Data Protection Act, 2023 adequately provide for corporate criminal liability in cases of data breaches, or does it primarily rely on civil and regulatory penalties?

4. How do the provisions of the Digital Personal Data Protection Act, 2023 interact with other Indian laws governing cybercrime and corporate accountability, including the Information Technology Act, 2000?

5. What legal and policy reforms are necessary to strengthen corporate accountability for data breaches in India?

Research Objectives

- To examine the concept, evolution, and principles of corporate criminal liability under Indian law.

- To analyse the legal framework governing data protection under the Digital Personal Data Protection Act, 2023.

- To critically evaluate whether the Digital Personal Data Protection Act, 2023 effectively addresses corporate criminal liability for data breaches.

Research Methodology

This study adopts a doctrinal legal research methodology based on the analysis of primary and

secondary sources. The primary sources include the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, relevant constitutional provisions, judicial decisions, and government reports. Secondary sources comprise books, journal articles, research papers, and legal commentaries on corporate criminal liability, cyber law, and data protection. The research employs an analytical and critical approach to examine the existing legal framework governing corporate liability for data breaches in India. The study is qualitative in nature and is confined to the Indian legal framework.

Evolution of Corporate Criminal Liability in India

- **The Legislative Foundation of the Information Technology Act, 2000**

India's first foray into cyberspace regulation began with the Information Technology Act, 2000, a law primarily designed to promote e-commerce and digital governance. Although the Act established civil and criminal penalties for unauthorized access and system damage, its focus was centred on technology rather than individual rights. For instance, Section 43 established civil liability for unauthorized access, while Section 66 criminalized specific cyber offenses.[6]

While these provisions addressed cyber misconduct, they failed to define data protection through the lens of informational privacy. Consequently, corporate entities handling personal data were governed largely by broad negligence standards, resulting in substantial accountability gaps.

- **Introduction of Section 43A and the 2011 Rules**

The enactment of Section 43A via the Information Technology (Amendment) Act, 2008, represented the initial effort to mandate data protection obligations for corporate entities. This provision established civil liability for organizations that, through the negligent implementation of security practices, caused wrongful loss or gain.[7] Subsequently, the 2011 Rules clarified these compliance mandates, addressing areas such as user consent, data retention constraints,

[6] Information Technology Act, 2000 (Act No. 21 of 2000), ss. 43 & 66.
[7] Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009), s. 43A.

and adherence to specific security standards.[8]

However, despite their forward-looking objectives, these regulations were hampered by both conceptual and practical flaws. The restricted scope of the "sensitive personal data" definition left out large volumes of information regularly handled by contemporary businesses.[9]

Furthermore, inadequate enforcement mechanisms and low compensation caps substantially weakened the framework's overall deterrent impact.[10]

- **Judicial Contributions Prior to Comprehensive Legislation**

Before the enactment of comprehensive legislation, judicial intervention played a limited but significant role in shaping India's data protection landscape. In Shreya Singhal v. Union of India, the Supreme Court stressed the necessity of safeguarding fundamental freedoms within the digital realm, advocating for precision and proportionality in cyber regulation.[11] While this ruling did not directly address data protection, it underscored the constitutional implications inherent in digital governance.

The definitive turning point occurred with the Puttaswamy judgment, in which the Court explicitly recognized informational privacy and highlighted the need to regulate private data processors.[12] This decision established the normative foundation for the DPDP Act and fundamentally altered the legal understanding of corporate accountability in the digital sphere.

Legal Framework Governing Data Protection in India

Under Section 43A, introduced via a 2008 amendment, a "body corporate" is liable to pay compensation if its failure to implement "reasonable security practices and procedures" results in wrongful loss or gain to any person. To implement this provision, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or

[8] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, r. 8.

[9] Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 97–101 (HarperCollins Publishers India, 2018).

[10] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* ¶ 2.19 (Ministry of Electronics and Information Technology, Government of India, 2018), available at: https://www.meity.gov.in, last visited on July 30, 2026.

[11] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

[12] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, ¶ 168.

Information) Rules, 2011 known as the SPDI Rules were enacted. These rules define "sensitive personal data or information" (SPDI) to encompass categories such as passwords, biometric data, and health records. Furthermore, the SPDI Rules mandate that companies maintain security standards compliant with recognized international benchmarks, such as ISO/IEC 27001, unless an alternative sector-specific standard is applicable.

CORPORATE LIABILITY UNDER THE DPDP ACT, 2023

The Digital Personal Data Protection Act, 2023, marks a significant shift in India's data governance, transitioning from the fragmented IT Act to a cohesive, rights-focused, and enforcement-oriented regulatory framework. By codifying the responsibilities of data processors, establishing formal oversight bodies, and introducing penalties for violations, the Act creates a robust compliance structure. Drawing inspiration from international standards like the EU's GDPR, the legislation has been specifically adapted to suit India's unique digital and socioeconomic landscape.[13]

This legislation primarily centres on three key stakeholders:

- **Data Principals** – These are individuals whose personal data is collected and stored.
- **Data Fiduciaries** – These refer to organizations that decide the purpose and methods for processing personal data.
- **Data Processors** – These are third-party entities that handle data processing activities on behalf of the data fiduciaries.

Key Responsibilities Placed on Corporations

The DPDP Act sets out several obligations that companies must follow when managing personal data. The main requirements are as follows:

- **Lawful and Consent-Based Processing (Sections 5–6):** Companies must obtain clear, informed, and voluntary consent from individuals before collecting or processing their sensitive personal data. Individuals must also have the right to

[13] Malavika Raghavan, "The DPDP Act: Promise and Pitfalls", 19 *Indian Journal of Law and Technology* (2023). x

withdraw this consent at any time.

- **Purpose Limitation (Section 7):** Personal data can only be collected for specific, legitimate purposes clearly communicated to the individual. Any further use of the data for different purposes requires additional consent.

- **Data Minimization (Section 8):** Organizations should collect only the minimum amount of personal data necessary to achieve the stated purpose, avoiding excessive or irrelevant information.

- **Accuracy and Storage Limitation (Section 9):** Data fiduciaries are responsible for ensuring personal data remains accurate and up to date, and must not retain it longer than necessary for the intended purpose.

- **Breach Notification (Section 16):** In the event of a data breach involving personal information, companies are required to report the incident to the Data Protection Board of India and inform affected individuals promptly and transparently.

- **Grievance Redressal (Section 14):** Organizations must set up internal mechanisms to address user complaints and resolve them within defined timeframes.

PENALTIES AND ENFORCEMENT

A major change from the previous IT Act is the establishment of the Data Protection Board of India (DPBI) as the central authority responsible for enforcing compliance and adjudicating violations. Penalties are detailed in Schedule I of the Act, including:

- Under Section 33, failure to prevent a personal data breach may result in fines of up to ₹250 crore.

- Processing children's data without adequate safeguards could lead to penalties of up to ₹200 crore.

- Repeated non-compliance or failure to uphold data principals' rights may incur fines of up to ₹150 crore.

- These financial penalties mark a significant departure from the weaker and

inconsistently applied compensation framework under Section 43A of the IT Act.

CORPORATE LIABILITY UNDER THE IT ACT, 2000

Under Section 43A, introduced through a 2008 amendment to the Information Technology Act, a "body corporate" is held liable for compensation if its failure to adopt "reasonable security practices and procedures" results in loss or wrongful gain to any individual. To give effect to this provision, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 commonly known as the SPDI Rules were issued. These rules specify what constitutes "sensitive personal data or information" (SPDI), including passwords, medical history, and biometric data. Companies are required to follow security standards aligned with internationally recognized frameworks such as ISO or IEC 27001, unless a specific sector has its own prescribed standard.

However, Section 43A[14] does not establish an independent data protection authority or a dedicated grievance redressal mechanism. Instead, disputes are handled by adjudicating officers appointed under Section 46 of the Act. Separately, Section 72A introduces criminal liability for unauthorized disclosure of personal information obtained through a lawful contract, done without consent or in violation of a confidentiality agreement. In practice, this clause has seen limited application, particularly against corporations, due to high evidentiary thresholds and complex legal processes.[15]

In *Karmanya Singh Sareen v. Union of India,*[16] petitioners raised concerns about privacy risks arising from WhatsApp's revised terms of service after its acquisition by Facebook, particularly its practice of sharing user data with Facebook and its affiliates. They contended that such data sharing occurred without clear user consent and adequate safeguards, violating the right to privacy and contravening Section 43A. The case underscored increasing public scrutiny over corporate data handling and revealed a gap between statutory obligations and real-world practices, especially in the absence of a strong enforcement body.

While the Supreme Court did not deliver a final ruling on the interpretation of Section 43A in this instance, it referred broader privacy questions to a Constitution Bench in the landmark K.S.

[14] Information Technology Act, 2000 (Act No. 21 of 2000), s. 43A.
[15] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), Gazette of India, Extraordinary, Part II, Section 3(i), May 25, 2011.
[16] *Karmanya Singh Sareen v. Union of India*, (2017) 10 SCC 1.

Puttaswamy case[16], where the right to privacy was ultimately recognized as a fundamental right under Article 21. Nevertheless, the Karmanya Singh Sareen case exposed structural shortcomings in the IT Act 2000, illustrating that individuals lacked a direct, effective remedy within the law and were forced to resort to indirect constitutional litigation to address data misuse.

The case thus acted as an important procedural and symbolic step toward calls for comprehensive data protection legislation. Although Section 43A was invoked, the proceedings made clear that the provision alone was insufficient to regulate the complexities of the modern data landscape without an empowered regulatory authority.

ZOMATO DATA BREACH[17]

In 2017, Zomato, one of India's top food delivery services, experienced a major data breach impacting around 17 million user accounts. The compromised information consisted of email addresses and hashed passwords. However, the company emphasized that payment details were not exposed, as they were stored in a separate system.

The breach reportedly stemmed from internal security weaknesses, which allowed an unauthorized individual to extract the data and subsequently list it for sale on the dark web. In response, Zomato reset passwords for affected accounts and released a public statement confirming the incident.

Legal and Regulatory Implications:

- At the time, India's Information Technology Act governed data protection. Section 43A required organizations to adopt "reasonable security practices" to safeguard user data. Despite this, no enforcement action was taken by regulatory or judicial authorities following the breach.

- Zomato asserted compliance with the ISO/IEC 27001 standard, a recognized benchmark for information security. However, the incident raised questions about how

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

[17] "Zomato Hacked: 17 Million User Records Stolen", *The Economic Times*, May 19, 2017, available at: https://economictimes.indiatimes.com/small-biz/startups/zomato-hacked-hackers-steal-data-of-17-millionusers/articleshow/58742044.cms?from=mdr (last visited July 31, 2026).

effectively such standards are implemented and monitored in practice.

- Notably, there were no penalties imposed on the company, nor was any compensation provided to users. This outcome reflects a key shortcoming of the IT Act: the absence of a strong, centralized enforcement mechanism.

AIR INDIA DATA BREACH[18]

In February 2021, Air India revealed a major data breach affecting approximately 4.5 million customers globally, including both Indian and international travelers. The incident stemmed from a cyberattack on SITA, a third-party provider responsible for handling passenger data systems for numerous airlines worldwide. Personal information exposed included names, passport details, booking records, frequent flyer data, and in some instances, credit card numbers though CVV codes were not accessed. While the breach occurred in late 2020, affected passengers were only notified in May 2021, prompting criticism over the significant delay in disclosure.

Legal and Regulatory Considerations

Similar to the earlier Zomato incident, this breach took place before the implementation of the Digital Personal Data Protection (DPDP) Act. At the time, India's IT Act lacked clear provisions mandating timely breach notifications, contributing to the prolonged silence. The involvement of SITA, an external data processor, further complicated accountability. Although Air India had contractual agreements requiring data safeguards, there was no effective enforcement mechanism under Section 43A of the IT Act to hold parties accountable for lapses.

Aadhaar Database Exposures[19]

Aadhaar, India's national biometric identification system managed by the UIDAI, collects and stores sensitive personal data such as names, addresses, fingerprints, and iris scans. Over the years, multiple reports of unauthorized access and weak security controls have raised serious

[18] "Air India Data Breach: Personal Info of 4.5 Million Leaked", *Business Standard*, May 22, 2021, available at: https://www.business-standard.com/article/companies/air-india-data-hacked-passport-credit-cards-and-otherdetails-leaked-121052101535_1.html (last visited July 31, 2026).
[19] Unique Identification Authority of India, *Aadhaar Act and Regulations*, available at: https://uidai.gov.in, last visited on July 31, 2026.

concerns about the privacy and integrity of this vast database.

Critical Analysis:

The breach underscored a significant disconnect between legal requirements and real-world enforcement. While Section 43A theoretically holds companies liable for failing to maintain adequate security especially when such lapses lead to loss or wrongful gain no formal proceedings were initiated against Zomato under this provision.

The SPDI Rules identify ISO/IEC 27001 as an example of acceptable security standards, yet mere certification does not guarantee effective protection. In this case, no investigation or adjudication was publicly recorded, and no complaints were filed under Section 43A by users or regulators.

This inaction highlights structural flaws in the IT Act, including the lack of a dedicated enforcement authority and a system that relies on individual victims to initiate complex legal processes through distant, often under-resourced officials. Despite the large scale of the breach, the absence of official scrutiny reveals the limitations of existing regulatory frameworks, particularly in holding powerful tech firms accountable.

The Air India breach highlighted two deeper structural issues:

- First, Indian legislation at the time offered insufficient clarity on the responsibilities and safeguards between data controllers and processors in contractual relationships.

- Second, the lack of mandatory breach notification protocols left individuals unaware and unprotected for months.

This case reinforced the urgent need for a dedicated data protection authority in India, along with clear procedural and jurisdictional guidelines to manage cross-border, third-party data processing arrangements.

Connection to the DPDP Act, 2023

Persistent Aadhaar data leaks, along with the landmark Puttaswamy Supreme Court judgment affirming the right to privacy, played a crucial role in shaping the Digital Personal Data

Protection Act of 2023. The new law introduces key obligations: entities must safeguard personal data, promptly report breaches, and face financial penalties for non-compliance, marking a significant step toward stronger data governance in India.

Recommendations

Based on the findings of this study, the following recommendations are put forward to improve corporate compliance and enhance the effectiveness of regulation under the DPDP Act:[20]

- **Clearer Regulatory Direction-** The Central Government and the Data Protection Board should develop sector-specific guidance outlining appropriate security measures, technical protections, and risk assessment methods. Defining clear criteria for identifying Significant Data Fiduciaries would help minimize ambiguity for businesses and support uniform enforcement of stricter requirements.

- **Strengthening Governance and Board Oversight**- Data protection responsibilities should be embedded within corporate governance structures, with oversight assigned to the board level. Measures such as appointing dedicated Chief Data Protection Officers, conducting routine cybersecurity assessments, and incorporating data protection performance indicators into executive evaluations can help translate legal duties into practical accountability.

- **Streamlined Cross-Border Data Transfer Rules**- Organizations should adopt standardized contractual arrangements and internal audit systems to manage international data flows. Promoting bilateral or multilateral agreements on data protection equivalence with major trade partners can ease compliance burdens and reduce legal complexities.

- **Building Independent and Capable Regulation**- The Data Protection Board's autonomy should be reinforced through transparent appointments, fixed terms, and requirements for technical qualifications. Training programs for Board personnel should emphasize expertise in emerging technologies, including artificial intelligence, cloud infrastructure, and distributed ledger systems.

[20] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), ss. 8, 9, 10, 16, 18 & Schedule I.

- **Promoting a Proactive Compliance Culture**- Regulators could introduce incentives such as reduced scrutiny or public acknowledgment for companies that consistently uphold high data protection standards. Widespread adoption of privacy-bydesign, ongoing staff education, and robust incident response planning should be encouraged across sectors.

- **Adapting Legal Frameworks to New Challenges**- Judicial bodies should offer clarity on the scope of fiduciary responsibilities, acceptable liability levels, and the appropriate scale of penalties. Legislative updates or supplementary rules may be necessary to address risks linked to AI-driven data processing, concentrated data control, and other evolving technological threats.

- **Fostering Public Trust Through Engagement**- Efforts to raise public awareness about data rights and responsible data use should be expanded. Collaboration with civil society, academic institutions, and industry groups can support the development of adaptive regulations, encourage ethical business practices, and help identify broader systemic vulnerabilities.

Conclusion

India's corporate sector now functions within a highly connected digital environment, where personal data has become a key strategic and economic asset. The Digital Personal Data Protection (DPDP) Act, 2023, establishes a legal framework designed to reconcile business innovation with the protection of individual privacy. Yet, its success depends on how effectively both regulators and companies adopt fiduciary responsibilities, implement strong governance mechanisms, and adapt to evolving technological threats. If managed well, this law can bolster not only privacy protections but also trust, competitiveness, and resilience in India's fastgrowing digital economy.

Further, DPDP Act marks a major advancement in India's data protection landscape by setting clear duties for Data Fiduciaries and creating a dedicated enforcement body the Data Protection Board of India. It enhances privacy safeguards through requirements for data security, breach disclosure, and significant financial penalties for violations. Nevertheless, this analysis reveals that the Act relies mainly on civil and regulatory enforcement and does not explicitly assign criminal liability to corporations for data breaches. As a result, serious cases of data misuse or

cybercrimes must still be addressed under existing laws such as the Information Technology Act, 2000.

Moreover, the impact of the DPDP Act will hinge not just on its legal provisions but also on consistent enforcement, institutional capability, and corporate adherence. While substantial fines may encourage better organisational accountability, persistent challenges remain in enforcement practices, governance standards, and corporate oversight. Improving institutional supervision, ensuring prompt reporting of breaches, encouraging privacy-conscious design in systems, and clarifying the legal responsibilities of companies and their executives would strengthen the current regulatory framework. A measured approach one that upholds individual privacy while promoting responsible corporate behaviour is crucial to building trust and accountability in India's expanding digital ecosystem.

REFERENCES:

- Rishab Dara, *Intermediary Liability in India: Chilling Effects on Free Expression*, Centre for Internet and Society (Apr. 2012), available at: https://cis-india.org/internetgovernance/intermediary-liability-in-india.pdf (last visited July 31, 2026).

- Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, Government of India, 2018).

- Rahul Matthan, *Privacy 3.0: Unlocking Our Data-Driven Future* 140–145 (HarperCollins Publishers India, 2018).

- Air India, "Important Information Regarding Cyber Security Incident", available at: https://www.airindia.com, last visited on July 31, 2026.