Page 4664 – 4669 **DOI:** *https://doij.org/10.10000/IJLMH.116533*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

The Legal Implications of Data Privacy and Security in Commercial Transactions

SEENATH P.S.[1], NEERAJA P[2] AND DHANALAKSHMI HARIKUMAR[3]

ABSTRACT

Due diligence on cybersecurity and privacy has become much more important in merger and acquisition (M&A) negotiations over the last 10 years. The days of presuming that only businesses involved in technology and innovation are affected by privacy and cybersecurity legislation are long gone. These days, data privacy and security laws in the US and other countries may apply to any firm that gathers personal data about its consumers, clients, workers, business representatives, and users even if that data is as basic as name, login, age, and password. In some M&A deals, a seller's adherence to existing data privacy and security standards can be crucial, and in some cases, a deal-breaker. This is particularly true when the seller's gathered personal data is one of the primary assets being sought after by a possible purchase.

Keywords: *CCPA - The California Consumer Privacy Act ; CPRA: The California Consumer Privacy Rights Act.*

I. INTRODUCTION

A component of data protection known as data privacy, or information privacy, deals with the appropriate handling, immutability, security, and storage of sensitive data. The appropriate management of personally identifiable information (PII), such as names, addresses, Social Security numbers, and credit card numbers, is generally linked to data privacy. The concept, however, also applies to other private or sensitive data, such as financial, intellectual, and health-related data. Vertical industry standards frequently oversee regulatory requirements of different governing bodies and territories, as well as activities related to data privacy and protection. The Supreme Court of India through its landmark judgement in the case of *K.S. Puttaswamy v. Union of India*[4] declared privacy as a fundamental right, and informational privacy, as a subset of right to privacy. In the age of big data, platforms gather enormous amounts of information that frequently consist of a range of information fragments, including bits of data that would not be considered "private in isolation" but when combined assist develop

[1] Author is a student at CSI College For Legal Studies, Kottayam, India.
[2] Author is an Advocate at High Court Of Kerala, India.
[3] Author is a student at CSI College For Legal Studies, Kottayam, India.
[4] *K.S. Puttaswamy v. Union of India,* W.P. (Civil) 494 0f 2012.

 [ISSN 2581-5369]

comprehensive behavioural profiles of specific people. Since digital markets are here to stay and any breach might result in serious consequences like identity theft, financial fraud, or the release of a person's private information, protecting consumer privacy is more important than ever (health records, sexual orientation, religion etc). The draught bill for India's data protection law was completed in 2019, but approval is still pending. The law is now being finalised. If the Personal Data Protection Bill is approved, it will establish the country's first cross-sectoral data protection legislative framework. The GDPR, which aims to provide its residents control over their personal data by recognising privacy safeguards including the right to be forgotten, has been referenced in the law. Like the GDPR in Europe, Indian legislation would also force digital companies to adopt privacy by design, get express consent before using personal data for most purposes, follow data minimization guidelines, and make it simpler for individuals to request that their data be erased. Although passing consumer data protection legislation is unquestionably a positive step, experts have warned that the draught as it stands gives the government the ability to circumvent regulations and could potentially give the government more control over the data of its citizens by allowing for broad exemptions based on public order or sovereignty. Therefore, it could be wise to include suitable protections, such as judicial review of government access, to prevent people' basic right to privacy. For the advantage of more domestic entities, the government-appointed committee on non-personal data has suggested making the exchange of non-personal data mandatory. It also suggests establishing new national laws and a new body to supervise its administration. The sector's level of competition will be significantly impacted by the eventual implementation of both laws. There is no one notion or method for data privacy. Rather, it's a discipline that includes policies, procedures, guidelines, and instruments to assist companies in establishing and upholding the necessary standards of privacy compliance. In general, data privacy consists of the following six components:

1. **Lawful structure:** Data privacy laws are examples of prevailing legislation that has been enacted and applied to data concerns.
2. **Policies:** Developed company guidelines and procedures to safeguard workers' privacy and that of user data.
3. **Practices:** Developed company guidelines and procedures to safeguard workers' privacy and that of user data.
4. **Affiliations with other parties:** any outside entities that deal with data, including cloud service providers.

 [ISSN 2581-5369]

5. **Data management:** Data access, storage, and security standards and procedures.
6. **Worldwide specifications:** Any distinctions or modifications to data privacy and compliance laws between international legal jurisdictions, including the United States and the European Union (EU).

II. WHY IS DATA PRIVACY IMPORTANT?

The financial value of data is closely correlated with the significance of data privacy. Businesses of all sizes are gathering and storing more data from more sources than ever before due to the developing data economy. There are several businesses uses for data, some of which are as follows:

- to recognise clients, ascertain their wants, and supply products and services to them;
- to comprehend, using information from networks and devices, the facilities, business infrastructure, and human behaviours;
- to extract knowledge from sources of data and databases; and
- to instruct AI and machine learning systems.

The goal of data privacy is to safeguard data from unauthorised access, theft, or loss. By practising good data management and limiting unwanted access that might lead to data loss, manipulation, or theft, it's critical to keep data private and safe. Individuals may experience identity theft, inappropriate account charges, or privacy invasion as a result of personal data exposure. Unauthorized access to sensitive data can negatively impact the results of data analytics and disclose trade secrets, intellectual property, and private conversations for enterprises. Data breaches, which are also known as data privacy violations, can seriously harm all parties concerned. People who are impacted by a data breach could discover hacked social media accounts, incorrect credit and financial activity in their name, and other problems. Significant regulatory repercussions for a corporation might include penalties, legal action, and irreversible harm to its image and brand. A firm may need to have a reaction strategy in place if it can no longer trust its data due to compromises in data integrity.

III. CHALLENGES OF DATA PRIVACY

Data privacy is neither simple or straightforward, and many companies find it difficult to comply with regulations and fend off attacks in a security and regulatory environment that is always shifting. Among the most significant obstacles to data privacy are the following:

- **Privacy is a secondary consideration.:** Business and technology executives often have

 [ISSN 2581-5369]

to grapple with data privacy issues long after they have established their IT infrastructure and business strategy, making it difficult for them to comprehend and handle the intricate requirements. Data privacy should be viewed as a primary business objective, and IT infrastructure, tools, rules, and training should all be created with the demands of privacy in mind.

- **inadequate data visibility:** When it comes to data privacy, the proverb "you can't manage what you can't see" holds true. Companies must have a thorough grasp of the types of data they have, how sensitive it is, and where it is kept. A company may then decide what security and data protection measures to take.
- **An excessive amount of data:** Petabytes of data made up of different files, databases, and stores spread over storage devices and cloud repositories may need to be managed by a corporation. Data may be easily lost track of, making it possible for sensitive material to evade security, privacy, and retention policies. To handle massive and expanding amounts of data, an organisation needs the appropriate tools and procedures.
- **More isn't always better:** Companies are beginning to realise that data needs context and value, and that keeping all of your data forever comes with costs associated with storage, protection, attack, and discovery concerns. The quantity of data gathered, it's worth to the company, and what constitutes acceptable retention demands must all be taken into consideration when creating modern enterprises' data retention policies.
- **An excessive number of gadgets:** Businesses in the modern day need to adopt technologies like wireless connectivity, BYOD, IoT, smart devices, and remote access. It gets more difficult to govern data storage and access while managing those devices with all these moving parts. In this complicated context, maintaining data privacy requires careful infrastructure management, robust access controls, thorough oversight, and thoughtful data governance regulations.
- **An excessive number of rules:** Regulations pertaining to data privacy may apply to a firm on a federal, state, provincial, or industry level. These existing restrictions also apply to a firm conducting business in another state, province, or nation. There are frequently new controls available, and they are subject to change. This results in a broad, intricate, and dynamic regulatory environment.

IV. BENEFITS OF DATA PRIVACY COMPLIANCE

Proper data privacy compliance can yield four major benefits for a business, including:

 [ISSN 2581-5369]

- **Reduced expenses for storage:** It can be expensive and dangerous to save all data indefinitely. Businesses that rationally choose what information to gather, how long to keep it, and how to put it all together save money on primary and backup data storage.
- **Improved data utilisation:** Time is of the essence for data. Timely and high-quality data may help a firm make better decisions about data collection and retention. This can lead to more accurate and pertinent analytical outcomes.
- **Improved brand recognition and business repute:** A company's reputation may be just as significant as its goods or services. Businesses that effectively implement and uphold data privacy policies may show that they value consumer information and data privacy, which enhances their reputation and builds their brand. On the other hand, a company's reputation and brand may be permanently harmed by a significant data breach.
- **Adherence to regulations:** A company can avoid lawsuits and penalties associated with data privacy violations by adhering to proper data privacy compliance.

V. PROTECTION OF DATA PRIVACY

There are countless guidelines and tips that can apply to data privacy. For individuals, data privacy can be reinforced with safeguards and actions such as the following:

- select strong passwords and change them frequently;
- use multifactor authentication (MFA) or biometric identification for important accounts;
- don't click links and buttons within emails;
- avoid providing PII that's unnecessary or not required;
- use malware tools and keep those tools updated; and
- use only trusted apps and websites.

For businesses, privacy principles and guidelines are more extensive and complex, but they can include the following tactics:

- collect as little data as possible to accomplish a business task;
- require strong authentication and MFA, such as user passwords or app credentials for APIs;
- understand data sources, uses and storage locations;
- employ access monitoring and logging to track data access;

 [ISSN 2581-5369]

- use encryption and other security technologies to protect data at rest and in motion;
- back up data and test restoration;
- ensure any third-party storage providers, such as cloud storage providers, share data privacy requirements and techniques; and
- regularly educate employees, partners and customers about data privacy guidelines.

A business must also contend with privacy legislation and regulatory issues related to data storage and retention. All data privacy guidance should include a thorough understanding of regulatory requirements.[5]

VI. CONCLUSION

Due diligence on privacy and cybersecurity may be crucial to the diligence process in M&A transactions, even in situations where the buyer is not acquiring the seller's collected personal information as the primary asset. This is because an increasing number of states and nations are attempting to adopt and implement data privacy and security regulations. Companies may still be subject to a variety of international, federal, and state privacy and data security regulations that affect their day-to-day operations, even though a seller might not be subject to some of the more comprehensive privacy laws, like the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Consumer Privacy Act (CCPA), the European Union General Data Protection Regulation (GDPR), or the California Privacy Rights Act (CPRA). Concerns about data security and privacy that may arise during an M&A transaction should be known to both the buyer and the seller.

*****

[5] Stephen J. Bigelow, Data Privacy (Information Privacy), TechTarget, https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy, (last accessed on DEC. 22, 2023, 10.33 PM)

 [ISSN 2581-5369]