ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]

VOLUME 4 AND ISSUE 1 OF 2025

APIS – 3920 – 0007 | ISSN - 2583-7230

Published by

Institute of Legal Education

https://iledu.in

INFORMATION SECURITY AND CUSTOMER DATA MANAGEMENT IN INDIA: THE ROLE OF LEGAL FRAMEWORKS

AUTHOR - THEJASVI CS* & DR.S. MARUTHAVIJAYAN**

* STUDENT OF TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY, CHENNAI, TAMIL NADU

** ASSISSTANT PROFESSOR OF TNDALU, CHENNAI, TAMIL NADU

BEST CITATION - THEJASVI CS & DR.S. MARUTHAVIJAYAN, INFORMATION SECURITY AND CUSTOMER DATA MANAGEMENT IN INDIA: THE ROLE OF LEGAL FRAMEWORKS, ILE MULTIDISCIPLINARY JOURNAL, 4 (1) OF 2025, PG. 1102-1108, APIS – 3920-0007 | ISSN - 2583-7230.

ABSTRACT:

Customer data management and protection have become essential to business operations, governance, and customer trust in the digital period. The quantity of personal data collected, processed, and stored by Indian businesses has expanded dramatically in tandem with the rapid growth of India's digital and practical services. This growth has created significant concerns about data privacy and information security. The current study looks into the legal issues of information security in Indian enterprises, with a focus on how Indian data protection regulations affect consumer data processing. The study examines at the evolution and impact of various significant components of regulations, notably the Sensitive Personal Data or Information (SPDI) Rules, 2011, the Information Technology Act of 2000, and the newly established Digital Personal Data Protection Act (DPDP) of 2023. It examines the extent that these legal and regulatory structures impact or restrict Indian business' data duties, especially in industries like information technology, banking, e-commerce, and healthcare. The research additionally assesses whether corporate governance, enforcement approaches, and regulatory compliance could enhance data for security policies. Small and medium-sized businesses often encounter difficulties with compliance because of difficulties with infrastructure, cost, or awareness, but many major corporations are adapting to the needs of the law. Customers are asking for more improved in privacy policies and transparency in company's operations, data handling and security of common people. The research identifies inconsistencies between legislative intent and actual execution utilizing a mixed – methods approach that includes legal analysis, case studies and privacy or primary data collected through researches of organization and customers. Then it looks into customer's knowledge and trust in legal safeguards for private data and information.

KEYPOINTS: Data Protection, Information Security, Digital Personal Data Protection Act (DPDP) 2023, Indian Businesses, Consumer Trust, Legal Framework.

INTRODUCTION:

Almost everything we do in the modern age of technology, especially banking, purchasing, socializing, traveling, even receiving medical treatment, involves giving away personal information online. Companies accumulate an immense amount of information about customers with the goal improve services, personalize experiences for customers, and expand their business. Names, telephone numbers, addresses, monetary details, and even confidential information like location or healthcare records can be comprised of this data. It's even more important than ever to keep this data confidential and protected as corporations focus more and more on digital technologies.

However, as data usage has increased, there have been data thefts, attacks via the internet, and the misuse of customer details. Numerous individuals are becoming increasingly concerned about how enterprises collect, safeguard, and make use of their personal information. They want to know whether their data has been handled responsibly and whether there are strong regulations in place to protect them if it is misused. A number of countries, including India, have established regulatory frameworks that specify how companies have to utilize and safeguard information about consumers with the goal to ease these worries. The Information Technology Act of 2000, the SPDI (Sensitive Personal Data or Information) Rules of 2011, and the most recent one, the Digital Personal Data Protection Act of 2023, are among the laws and regulations in India that are designed to protect data security and privacy. These regulations specify how companies must handle personal data, including how it must be gathered, saved, processed, and distributed.

The purpose of this study is to investigate the relationship between different Indian regulatory frameworks and how companies handle client data. It will investigate how regulations impact corporate operations, how well-informed consumers are about their data rights, and if current laws are effective in preventing the exploitation of personal data. In order to comprehend the practical effects of these regulations, it will also examine case studies, official government sources ,and survey data .There has never been a greater need for robust information security measures supported by legally binding regulations as India's digital economy continues to expand. In order to create a safer digital future for companies and consumers alike, this paper aims to provide insights into where India stands today, what obstacles still need to be overcome, and what advancements may be made.

STATEMENT OF PROBLEM:

1. This research states how companies handle personal data of customers, as they collect a huge amount of information from them.

2. Though legal acts like and IT act (Information Technological act 2000), SPDI rules (Sensitive Personal Data and Information Act 2011) and DPDP act (Digital Personal Data Protection Act 2023) are there, many businesses- especially small and medium industries find difficult to comply all of them.
3. Major amount of common people doesn't know about the legal regulations and acts and about how their personal data is collected, utilized and stored by companies.
4. The implementation of data protection rules is still evolving, and regulatory monitoring is frequently limited or delayed in reaction to data breaches.

REVIEW OF LITERATURE:

1. The Information Technology Act of 2000 and its Section 43A, which holds businesses responsible for their failure to take acceptable security measures, have been extensively examined by academics. Law schools and technical universities like NLSIU,IIM and IIT have legal research on data protection laws and cybersecurity.

2. The Digital Personal Data Protection Act of 2023's Inception India's first comprehensive privacy law, the Digital Personal Data Protection (DPDP) Act, 2023, has drawn notice. MeitY (2023) says that the DPDP Act establishes basic principles such as the right of users to access and remove data, consent-based gathering of data, and data minimization. Although there are implementation and awareness issues, legal experts like Sharma (2023) point out that the Act moves India closer to international data protection norms like the EU's GDPR.

3. Large firms like KPMG, Deloitte, EY, PwC AND Cyber security firms are starting to implement

more robust safety policies, but small and medium-sized businesses (SMEs) find it difficult to comply because of a lack of finances, technological knowledge, and regulatory clarity, according to studies (KPMG Report, 2021). Only 35% of Indian companies were entirely prepared for data privacy audits, according to a NASSCOM poll from 2022, revealing a compliance gap.

4. According to a number of assessments and publications by Nishith Desai Associates, Trilegal and Cyril Amarchand Mangalas, Indian consumers are still not well-informed on their data rights. More than 60% of Indian users did not read privacy policies, and most were not aware of how their data was being gathered or utilized, according to a survey conducted by the Internet and Mobile Association of India (IAMAI, 2020). The effectiveness of data protection legislation in practice is called into question by this discrepancy between legal rights and public knowledge.

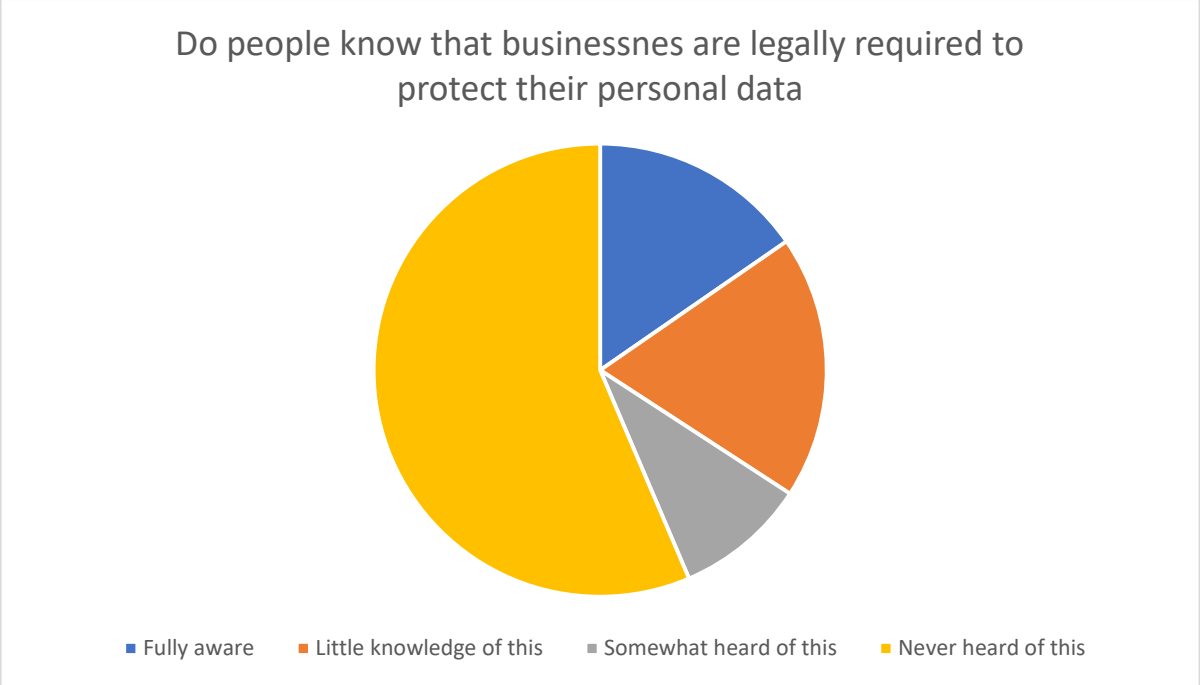
5. Numerous government papers have looked at the role that law enforcement and the Indian Computer Emergency Response Team (CERT-In) play in combating cyberthreats. Even though India's systems for reporting cyber incidents have improved, research from the ORF (Observer Research Foundation, 2021) indicates that there is still ineffective coordination between companies, authorities, and enforcement agencies.

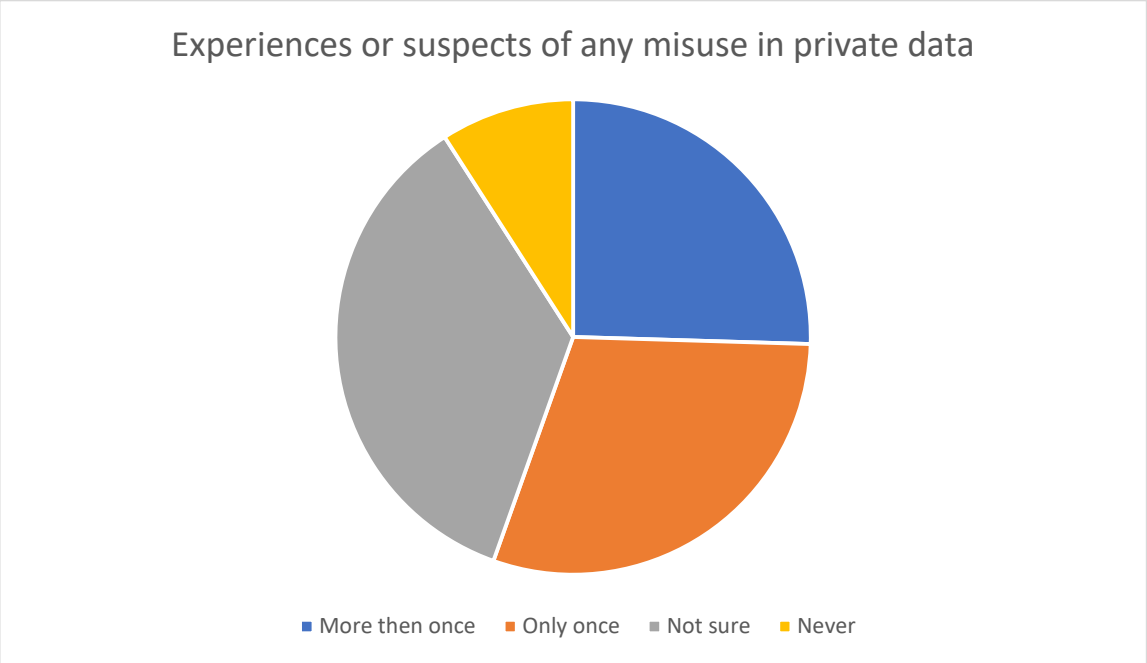
METHODOLOGY:

- Both quantitative and qualitative data are included in this study. Quantitative data(from survey responses)they are calculated using percentage distributions and data visualizations (pie chart)
- Students and people who are knowledgeable about how businesses handle consumers personal data—since they gather a great deal of information from them—as well as the legal framework surrounding this—were asked questions and completed surveys to gather both primary and secondary data for this study. Primary data used: Tools used are google forms, Questions are open ended questions, mostly Yes or No questions with clarity and ease. Totally 12 questions. Secondary Data were taken from official legal documents, reports from industrial bodies, academic journals and research papers. And totally 100 respondents answered their different and honest opinions.

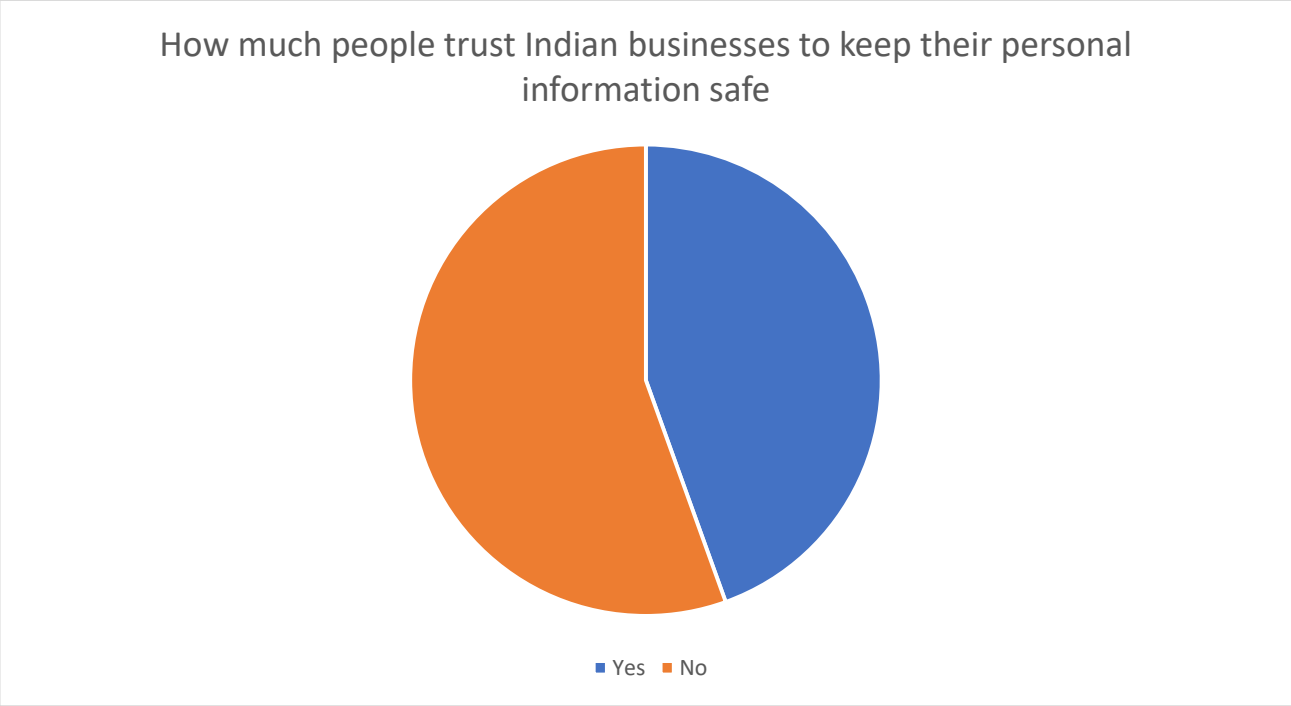
ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in

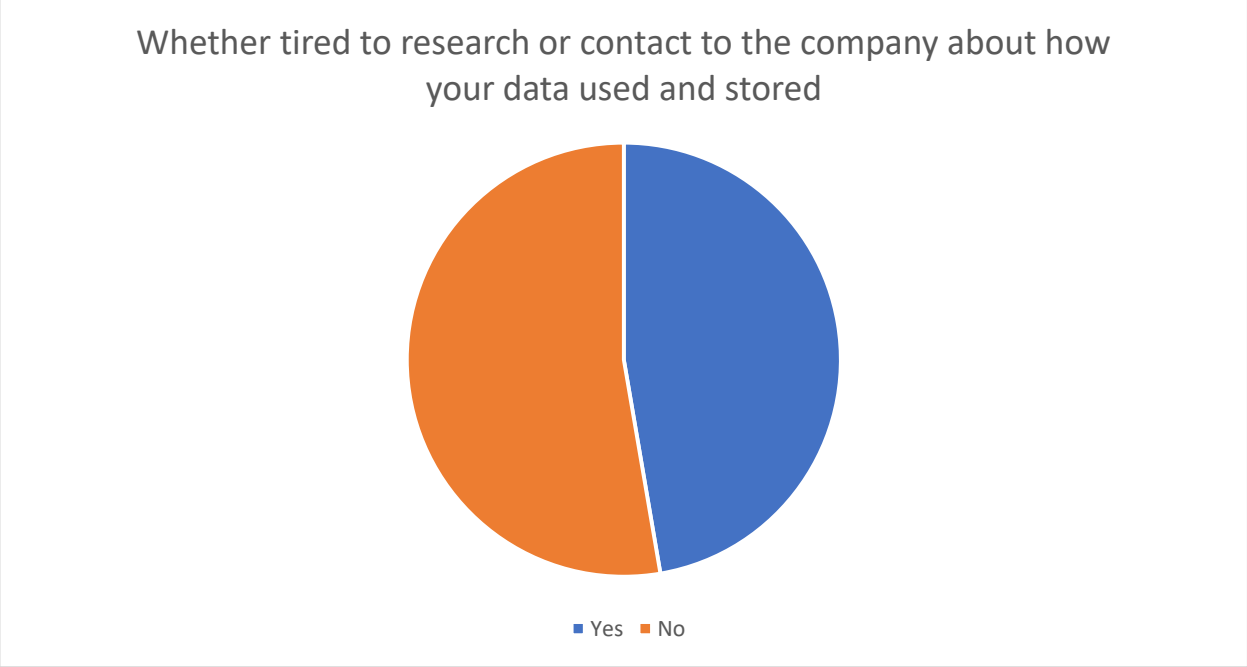
RESULTS AND DISSCUSSION:





ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 1 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in





The responses to the survey reveal that while data privacy is an emerging concern among Indian customers, there is a significant lack of awareness about the legal obligations of businesses under Indian law. A majority of the respondents admitted to having little or no knowledge of the legal requirement for businesses to protect personal data.

Most participants also confessed to not reading privacy policies before sharing personal information, indicating that current policies are either too complex or not emphasized enough by companies. Interestingly, a large number of respondents had, at some point, refused to share their personal data due to uncertainty about how it would be used—showing that people are cautious even if they are not legally informed. Trust in businesses appeared divided; while some respondents expressed confidence, others did not trust companies to safeguard their information. Although most had not

personally experienced or identified misuse of data, a few had encountered issues more than once, while many were simply unsure.

Nearly all participants agreed that businesses should be held legally accountable for misusing data, with varied opinions on the degree of punishment based on the severity of harm. Additionally, most believed that privacy policies in Indian businesses should be improved, and only a small number had taken the initiative to contact companies or research how their data is handled. The final suggestions strongly emphasized the need for increased public awareness and transparency, as many participants felt that privacy laws and policies should be known and easily understood by everyone. These findings highlight the critical need for legal literacy, stronger enforcement of data protection laws, and better communication between businesses and customers.

The survey responses are strongly related to the research issue, demonstrating a significant gap between the presence of data protection regulations in India and their practical use. While regulatory frameworks try to protect customer data, most consumers are uninformed of their rights and privacy rules, and many distrust organizations' data activities. This demonstrates that legal measures alone are insufficient without proper execution, public knowledge, and company accountability—exactly the issue the research attempts to address.

CONCLUSION:

The rising digital revolution in India has resulted in a considerable increase in personal data acquired by corporations across all sectors. While regulatory frameworks such as the Information Technology Act of 2000 and the more recent Digital Personal Data Protection Act of 2023 seek to secure customer data, this analysis finds a significant gap between these laws' aims and their execution on the ground. The poll done as part of this research emphasizes several important realities: Most consumers are either unaware of or have a limited understanding of the legal responsibility that firms have in managing personal data. Despite legislative safeguards, customer trust remains fragile, and awareness of privacy policies and rights is disturbingly poor.

The statistics also show that a sizable proportion of customers do not read privacy policies, and relatively few actively seek to understand how their data is maintained or utilized. However, there is a palpable worry among customers about how their personal data is handled, with many expressing reluctance or unwillingness to submit information when they believe their privacy is threatened. Trust in businesses is divided, with some respondents feeling secure while others are skeptical, particularly over data sharing with third parties or superfluous permissions requested by apps and platforms. Most importantly, virtually all participants believed that corporations that misuse customer data should face legal consequences, demonstrating the public's strong support for accountability.

From the perspective of law, these responses corroborate the research hypothesis that existing rules, while well-intentioned, lack practical visibility, awareness, and strict enforcement mechanisms. According to the report, customers expect privacy policies that are more open, streamlined, and easily available. These findings underline the importance of not only strong legal frameworks, but also active government activities to enhance data protection awareness, ensure firms meet compliance standards, and provide more options for consumer grievance redressal.

Finally, the study indicates that, while the Indian legal system has made significant progress in data protection, much more work remains to be done to bridge the gap between law and real-world behavior. Future changes should prioritize public education, company accountability, and regulatory openness to guarantee that customer data is not only legally protected, but also appreciated and secured in practice. The

success of any legal framework is determined not only by its formulation, but also by its ability to be understood, obeyed, and enforced—which remains the most significant obstacle for India's data protection ecosystem today.