International Research Journal of Commerce and Law
Volume 11 Issue 10, Oct 2023 ISSN: 2349-705X Impact Factor: 7.893
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

CUSTOMERS' RIGHT TO DATA PRIVACY IN THE INDIAN BANKING INDUSTRY: A LEGAL ASPECT

Jai Govind Pancholi

Seedling School of Law & Governance,

Department of Law, Jaipur National University

ABSTRACT

The banking industry has long recognized the importance of privacy in regards to the collection, protection, and use of consumer financial information. Prior to the enactment of laws, large banks had long been implementing their own privacy policies. Furthermore, some banking consortiums have jointly agreed to implement a set of privacy principles to ensure the public's trust in the security and reliability of financial transactions. A comprehensive examination was carried out on diverse laws, legislation, and challenges pertaining to data privacy inside the government. As a result of this research, alternative conclusions were formulated based on the observed facts.

KEYWORDS: -Customer rights, Data protection, banking industry, Laws and legislation.

INTRODUCTION

India is the global leader in terms of population size, being home to almost 1.2 billion people and also being a democratic nation. The nation functions under a national-level parliamentary system, distinguished by the existence of many political parties and two legislative chambers. In the past two decades, the Indian economy, formerly characterized by government control, has witnessed the emergence of a dynamic private sector. With the eleventh largest global economy, it is presently the second fastest-growing major economy. Moreover, it functions as a prominent global hub for the outsourcing of personal data processing, particularly in industries such as telecommunications contact centers and the transcription of medical consultation notes. In order

to gain a comprehensive understanding of a nation's data protection legislation, it is crucial to consider the surveillance mechanisms already employed within that jurisdiction. The Indian government has been granted the authority to intercept messages in situations involving a national emergency or when it is necessary to ensure public safety. However, the restrictions put in place by the Supreme Court in 1996 restrict the use of phone tapping. These regulations specify the conditions and grant permission to individuals to carry out such actions.

Critics have raised concerns about the expansive authority bestowed upon law enforcement agencies by the recent 'anti-terrorism' legislation, enabling them to detain anyone suspected of terrorism, monitor communications, and curtail freedom of speech. However, these statutes incorporate audit procedures that involve judicial examination and parliamentary oversight. The Indian judiciary strictly enforces restrictions on searches conducted without a warrant. The banking sector is largely acknowledged as a crucial cornerstone for both economic and social progress. The modern banking business must prioritize both robust data analytics and stringent privacy protection. Ensuring the maintenance of clientele, fostering confidence, and securing long-term sustainability are of utmost importance. In recent years, there have been notable legal advancements and court decisions concerning data protection, aimed at adhering to the mandate of the Information Technology Act 2000 [ITA 2000] to prevent illegal access to customer data. Nevertheless, a comprehensive examination of Indian data protection and privacy legislation uncovers certain notable obstacles that need to be addressed prior to considering the country as having a legal framework that conforms to international norms. Several protections now lack functionality due to either a lack of crucial legislation or non-compliance with the laws. The data protection architecture in India exhibits deceptive features and, at most, can be regarded as a commitment to future enhancements.

Data privacy of customers in banking sector

In today's world, financial institutions make use of big data technologies in order to collect, store, and examine massive amounts of financial data derived from a wide variety of sources and presentation styles. Because of this, they are able to glean useful information and improve the

capabilities of the various financial services offered by the business. [Huo, H., and other authors, 2023]

The major worry that consumers have is the possibility of their data being misused or their privacy being violated. People who use financial apps or third-party software for financial services have to agree to privacy policies or give different permissions for information to be collected or retrieved. This is because digital consumption is growing so quickly. This is the case regardless of whether they use the program themselves or not. The background system logs all of the information that an online user enters, including their identity, location, shopping preferences, payment passwords, and any other pertinent information. Misuse and disclosure of sensitive financial information occurs all too regularly, and it frequently occurs as a result of practices such as excessive marketing and discriminatory pricing based on big data. The most significant threat that financial institutions face is the loss of customer data. Insiders can be bribed to illegally sell or purposefully divulge information, or they can get aid from hackers to facilitate data leakage, both of which can lead to financial losses when the market performs below expectations. Alternatively, hackers can help insiders facilitate data leaks. In addition to this, there is the possibility that the data will become corrupted. During digital transactions, the absence of labels in the data renders it susceptible to unlawful copying and change. The outputs of the model will be considerably disrupted in the event that the data sample is purposefully tampered with. This can result in significant costs for financial institutions related to the cleaning of their data, and it can also have an effect on the decision-making procedures at such institutions [Sun et al., 2019].

By asserting that privacy is a basically contested notion, we contend that the disputes around privacy and the resulting ambiguity in its interpretation are crucial in determining its fundamental nature and necessary for its proper operation. Privacy concepts are in conflict with each other in both theoretical and practical aspects. This indicates the applicability of Gallie's theory in this field to the extent that, as Garver points out, concepts are primarily contested as a result of their usage in essentially contested arguments. According to Garver E. (1990), on page 258, it is suggested that partisans, rather than theorists, are the ones who assess if a conflict

involves a concept that is essentially contested. The citation for this information is found in Garver E.'s work from 1990, on page 258. [Reference: Garver, E. (1990)]

Consent management of consumers

Customer consent must be voluntary, tailored to the intended data usage, informed, unambiguous, and revocable at any time. Obtaining client consent for new services can be challenging, particularly when their data will be disclosed to external entities. It is common for a new and creative idea to encounter obstacles when there is insufficient support and consent from a significant number of clients. It is crucial to highlight the customer's ability to revoke their consent at any given time. Consequently, it is necessary to establish data governance mechanisms to enable the removal of such material. Teams specializing in technology, business, user experience, and compliance should take charge of the consent management function to avoid using unnecessarily complex or discouraging terms. Several prominent financial services firms have hired dedicated data relationship managers to effectively communicate signals to customers in a manner that is both valuable and easily understandable.

AIin banking sector

The use of artificial intelligence in the banking industry raises substantial concerns over data privacy, as highlighted by the Financial Stability Board in 2017. The bank's reliance on external service providers to safeguard consumer data privacy is uncertain due to the ongoing development of legislative frameworks (Truby, Brown, and Dahdal 2020). The utilization of AI-powered technologies, such as customer service chatbots or natural language processing (NLP) for assessing staff and customer interactions, has the potential to infringe upon individuals' privacy (Caldwell et al., 2020; Lai, Leu, and Lin, 2018). The regulatory framework is always changing. This ambiguity may impede the institutions' ability to effectively address cybersecurity risks. The data suggests that trust, innovativeness, familiarity, and knowledge level are key factors that contribute to the higher adoption of e-banking in India. Customers are willing to utilize internet banking, despite their apprehensions regarding security and privacy, as long as

banks furnish them with sufficient guidance. Neha Dixit and Dr.Saroj K. Datta collaborated in 1970.

Data privacy laws

The majority of countries globally have legislation regarding privacy. The implementation of these privacy measures has empowered governments to establish additional legislation that acknowledges individuals' entitlements to their data. The regulations revolve around a set of principles that establish the procedures for gathering, exchanging, and processing personal data. Notwithstanding these regulations, data generators, including consumers and small and medium-sized organizations (SMEs), lack ownership rights over the data they generate and are unable to fully capitalize on its use (Solove, 2013). India lacks codified data privacy legislation comparable to the data privacy laws in the United Kingdom and the European Union, which establish the requirements for safeguarding data privacy by individuals and organizations. In India, the Information Technology Act, 2000 ('the IT Act') and its associated laws are applied to ensure the protection and confidentiality of specific sensitive data and personal information. The Personal Data Protection Bill, 2019 ('the Bill') is now under review and consideration by the Lok Sabha, the lower house of the Indian Parliament. If passed, the bill would establish comprehensive data privacy legislation in the country.

Article 21 of the Constitution of India grants individuals the right to privacy. In a specific case, the Supreme Court of India acknowledged India's international legal obligations and affirmed that the right to privacy is an inherent and essential right derived from the right to life as guaranteed by the Constitution [India: Data Protection in the Financial Sector (2021)]. The benefits derived from the exchange of personal data are not fully recognized and are not fully utilized on an individual basis. This is particularly accurate when it comes to consumer loans. The Indian government has formed a Committee of Experts to analyze the different difficulties related to data protection in India and create a Data Protection Bill.

Ensuring client information privacy is a crucial aspect of the Client Protection Framework due to its inherent importance in a world that heavily relies on information. The impact of globalization on an individual's privacy is becoming evident. The prevalence of data breaches is increasing due to the growing transfer of personal information across international borders, potentially resulting in financial fraud.

Challenges faced by banks in protecting data

The presence of data privacy laws and the potential damage to one's reputation resulting from data breaches necessitate the implementation of a strong data privacy policy. Data privacy in the financial services industry in 2023 The 4V characteristics of big data present distinct challenges for the fields of management, analytics, finance, and other diverse applications. The difficulties encompass the efficient organization and management of banking sectors, the discovery of innovative business models, and the resolution of conventional banking problems [Sun, Y et al., 2019]. The future of development will be significantly disrupted by data-driven methodologies. Historically, banks have prioritized the accumulation and retention of vast quantities of data. Nevertheless, they encounter substantial obstacles when considering the complete utilization of such data. This article provides a concise overview of the major obstacles faced by the banking sector in the age of big data, taking into account its distinctive features.

Regulation of data

The current legislative framework for protecting personal data, which was established during the early stages of computer and ICT development, is no longer viable. This is primarily due to the significant technological advancements of the past decade, which have led to a substantial transition from offline to online activities. Additionally, the increasing importance of data as a valuable resource and the integration of data processing into daily routines have further complicated the matter. Hence, European lawmakers have reached a consensus to substitute the outdated Directive 95/46/EC with a legal tool that is better equipped to tackle the current and future aspects of data processing. Regulation 2016/679, commonly referred to as the General

Data Protection Regulation, or GDPR, came into effect on May 25, 2018, after a lengthy legislative procedure. It was finally implemented earlier this year. The implementation began on May 24, 2016, but data controllers are not obligated to adhere until May 25, 2018. The primary objective of the new regulation is to eradicate perplexing national transposition rules and provide a harmonized European legal framework for data protection by directly and consistently applying it to all Member States. The Regulation maintains the exceptions outlined in the Directive, which allow for such choices to be taken in relation to the formation or execution of a contract or when authorized by law. Furthermore, the GDPR allows for automated determinations on the condition that the data subject has explicitly consented. In such a situation, the controller must include safeguards that enable data subjects to receive human assistance, express their views, and object to the decision. Automated decisions, on the other hand, should not rely on specific data types.

Implementation of data protection regulation

The current legislative framework for protecting personal data is inadequate due to the rapid technological advancements of the past decade. These advancements have led to a significant shift from offline to online activities, the increasing value of data as a commodity, and the integration of data processing operations into daily routines. Therefore, European legislators have unanimously agreed to replace the obsolete Directive 95/46/EC with a legislative instrument that is more capable of addressing the present and future dimensions of data processing. Regulation 2016/679, commonly referred to as the General Data Protection Regulation, or GDPR, came into effect on May 25, 2018, following an extensive legislative procedure. It was finally implemented earlier this year. The implementation began on May 24, 2016, while data controllers are not obligated to adhere until May 25, 2018. The primary objective of the new regulation is to eradicate convoluted national transposition legislation and provide a harmonized European legal framework for data protection that will be universally applicable to all Member States. The Regulation upholds the exceptions outlined in the Directive, which allow for such decisions to be made in relation to the signing or execution of a contract or when authorized by law. Furthermore, the GDPR allows for automated choices, on

the condition that the data subject has explicitly granted their consent. Under such circumstances, it is imperative for the controller to incorporate protective measures that allow data subjects to access human support, articulate their opinions, and raise objections to the decision. Automated decisions, on the other hand, should not rely on specific classifications of data.

Nevertheless, ensuring the security of storage is a continuous and ongoing endeavor. Irrespective of the location of the data, it is imperative to ensure its protection as an integral component of a comprehensive business plan. Many firms utilize storage area networks (SANs) as a means of data storage. IT teams should take into account the following factors when developing a security strategy:

- Unauthorized individuals should encounter significant obstacles while attempting to infiltrate the storage network, while authorized users and programs should experience seamless access.
- The network must exhibit reliability and consistency in the face of diverse usage patterns and environmental circumstances while ensuring its security remains intact.
- The network's integrity and robustness should be unaffected by internet threats such as viruses and other malicious software.

IT teams tasked with storage security are responsible for completing numerous procedures to guarantee data protection. Implement robust key management protocols to ensure security, and employ encryption for sensitive data during transmission and storage. In order to mitigate potential security vulnerabilities, it is advisable to disable any services that are not essential. Regularly implement security patches and operating system updates. Implement robust network security protocols to deter unauthorized individuals from gaining access to storage systems and the sensitive data they contain. Implement storage and data redundancy as a precautionary measure against hardware malfunctions, criminal activities, or natural disasters. Ensure user comprehension of the policies and procedures governing their utilization of the network, storage, and data.

Practical implications

Our research offers a foundation for enhancing the data security of universities and other scientific research institutes in the higher education sector. This has important practical consequences for universities that want to mold their data security strategies in order to reduce the likelihood of data breaches. To begin, regular system maintenance and finding and fixing technological holes as soon as they are found can help create a safer and more stable information space by limiting the number of ways attackers can get in. Second, increasing the fluidity and openness of data is a factor that can contribute to the production of more valuable data. Third, in the process of adopting new information technologies like cloud storage, educational institutions may want to evaluate the risk of data breaches caused by various types of services, thereby assessing the pros and cons of the situation. Fourth, increasing the rigor of data security training and elevating key personnel's understanding of the importance of data security can help prevent problems and information leaks caused by human errors before they occur.

CONCLUSION

The banking sector has undergone a substantial shift from conventional physical branches to contemporary data-oriented financial organizations. The emergence of big data technologies has driven this transformation, allowing banks to examine extensive volumes of data to enhance their decision-making processes. Based on the research findings, the primary barriers to achieving effective data privacy during analysis are insufficient training and the absence of a well-defined policy. Subsequently, there is a dearth of dedication from upper-level administration, inadequate safeguarding of storage, and unrestricted entry. They possess extensive knowledge regarding the utilization of customers' personal information in analysis, as well as the utilization of such information by their bank. Additionally, they are well-versed in the implementation of proper outsourcing policies by banks to prevent and limit any unauthorized access to customer data. Therefore, the data privacy rules in India, although currently restricted in scope and depth, adhere to the fundamental principles established in the Puttaswamy case. All data disclosure requests made by statutory or regulatory agencies will be governed by the same rules.

Companies make significant efforts to ensure compliance with the General Data Protection Regulation, but there is still a gap between their strategic plans and their actual implementation. This gap becomes more evident as organizations carry out assessments, formulate goals, and establish frameworks, yet they appear to overlook the actual information technology. There is data indicating that this limitation arises from the prioritization of communication operations, the absence of technology skills, and a simple lack of time for practical implementation. The future of big data in banking presents certain hurdles, but the potential for significant and revolutionary change is considerable. Financial institutions that can efficiently utilize the potential of big data will be in a stronger position to fulfill the changing requirements of their customers and thrive in a progressively competitive environment.

REFERENCES

1. Garver E. 1990. Essentially contested concepts: the ethics and tactics of argument. *Philos. Rhetoric* **23**, 251–270. See http://www.jstor.org/stable/40237644
2. Sun, Y.; Shi, Y.; Zhang, Z. Finance Big Data: Management, Analysis, and Applications. *Int. J. Electron. Commer.* **2019**, *23*, 9–11
3. Huo, H., Guo, J., Yang, X., Lu, X., Wu, X., Li, Z., Li, M., et al. (2023). An Accelerated Method for Protecting Data Privacy in Financial Scenarios Based on Linear Operation. *Applied Sciences*, *13*(3), 1764. MDPI AG. Retrieved from http://dx.doi.org/10.3390/app13031764]
4. S Chatterjee, *Data Privacy a Fundamental Right in India? An Analysis and Recommendations From Policy and Legal Perspective*, 61 International Journal of Law and Management 170-190 (2019)..
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

6. [1]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
7. *India: Data protection in the financial sector*. (2021, September 1). DataGuidance. https://www.dataguidance.com/opinion/india-data-protection-financial-sector
8. Electronic Privacy Information Centre (EPIC) and Privacy International (editors), *Privacy and Human Rights*, 10th edn (2006), at 547, available at <http://epic.org/phr06/PHR, 2006: 547>.
9. Truby, J., R. Brown, and A. Dahdal. 2020. Banking on AI: Mandating a proactive approach to AI regulation in the financial sector. *Law and Financial Markets Review* 14 (2):110–20. doi:10.1080/17521440.2020.1760454.
10. Caldwell, M., J. T. A. Andrews, T. Tanay, and L. D. Griffin. 2020. AI-enabled future crime. *Crime Science* 9 (1):1–13. doi:10.1186/s40163-020-00123-8.
11. Lai, S. T., F. Y. Leu, and J. W. Lin. 2018. A banking chatbot security control procedure for protecting user data security and privacy. In *International conference on broadband and wireless computing, communication and applications* (561–71). Springer, Cham, October
12. Financial Stability Board. 2017. Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. Financial Stability Board Research Paper, https://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/.
13. Data privacy in the financial service industry(2023). Capgemini.com. Retrieved January 20, 2023, from https://www.capgemini.com/wp-content/uploads/2017/07/Data_Privacy_in_the_Financial_Services_Industry.pdf
14. Information and Technology Act, Section 43A and 72A (2000).
15. Neha Dixit &Dr.Saroj K Datta, *Acceptance of E-Banking Among Adult Customers: An Empirical Investigation in India*, 15 The Journal of Internet Banking and Commerce 1-17 (1970).