INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DATA PRIVACY AND PROTECTION IN BANKING AND INSURANCE

AUTHOR - DIVYANSHU BHARTI* & DR. AMIT DHALL**

*STUDENT OF LAW, AMITY LAW SCHOOL, NOIDA, UTTAR PRADESH

** FACULTY OF LAW, AMITY LAW SCHOOL, NOIDA, UTTAR PRADESH

BEST CITATION - DIVYANSHU BHARTI & DR. AMIT DHALL, DATA PRIVACY AND PROTECTION IN BANKING AND INSURANCE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (4) OF 2025, PG. 226-236, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The increasing digitization of banking and insurance products and services has made data privacy and protection a high-priority topic. The Financial Institutions storages millions of tons of sensitive customer-related data, such as account information, personal details, and transaction history. This data can be easily manipulated with cyber-attacks, unauthorized access, and data breach; hence strengthened security is needed to safeguard it. Internationally, there exist certain regulations such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Basel Committee on Banking Supervision (BCBS), which define international data protection standards. In the Indian context, financial institutions are subjected to data privacy practices by Information Technology Act, 2000; the proposed Personal Data Protection Bill (PDPB); and guidelines issued by Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDAI).

Although strict laws and regulations exist, the challenges faced by financial institutions still remain. Some of these challenges include cyber threats, compliance with changing laws and regulations, risks pertaining to third parties, and a balancing act between security and customer convenience. Cyber threats such as phishing, ransomware attacks, and data breaches pose floodgates to secure banking and insurance data. Hence, the institutions should be installing strong cybersecurity standards, which may include encryption tools, two-factor authentication, and regular audits. Secure data storage, being compliant with regulations, customer awareness programs, and strong third-party risk management are some of the other strategies that need to be added. Informing consumers about phishing scams and frauds will help in creating an additional layer of defense towards securing data.

1. Introduction

Digital transformation of the banking and insurance industries has greatly impacted financial services; in other words, increased efficiency, access, and convenience for customers. Digital platforms facilitate transactions seamlessly, allow personalized offer management services, and promote financial inclusion[319]. However, the same transition has begun to open the floodgates to enormous risks relating to data privacy and security. Increasing reliance on digital technologies draws in cyber-attacks, unauthorized access to data, and breaches against financial institutions, thereby making data protection a critical agenda[320].

Data privacy has now become a sine qua-non for any financial entity to make an impression on the minds of consumers with trustworthiness, as well as a must for compliance[321]. Financial

[319] See generally, *Chris Skinner, Digital Bank: Strategies to Launch or Become a Digital Bank* (1st edn, Marshall Cavendish International 2014) 5-10.

[320] *Daniel T. Stabile et al., Digital Assets and Blockchain Technology: US Law and Regulation* (1st edn, Edward Elgar Publishing 2020) 23.

[321] *World Economic Forum*, 'The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services' (August

institutions manage massive amounts of sensitive data, including but not limited to personally identifiable information (PII), financial records, and details regarding transactions[322]. Any breach or misapplication of this information could result in punishingly expensive consequences, both financially and in terms of reputation[323]. To add insult to injury, numerous regulatory bodies throughout the world have enacted stringent data protection laws that protect customer information, and allow for the prosecuting of any organization found in serious non-compliance[324].

This study responds to questions about whether banking and insurance WiFi providers observe data privacy, highlighting the existing law and practices in use around the globe within the financial institutions to advance on data security. In this respect, it addresses the international and national regulatory frameworks of concern, the major bottlenecks to the financial institutions, and the risk management strategies employed by the said institutions. Knowledge in this regard enables institutions to upgrade their cybersecurity frameworks and bolster consumer trust in the digital provision of financial services.

2. Importance of Data Privacy in Banking and Insurance

Banks and financial institutions typically amass and keep massive quantities of private and financial data about individuals, including their account information, credit histories, medical records, and transaction patterns. This information is valuable and lucrative to cybercriminals. Therefore, endangering such information usually leaves the way open for facilitating financial crime such as fraud, identity theft, and theft, and unauthorized transactions. The consequences are so dire that even one breach may have the potential to compromise the customer records of millions, causing tremendous financial impacts, detriment to reputation, and legal liabilities[325].

More so, data privacy measures go a long way in instilling consumer confidence-in-people rather expectedly expect security in handling their money information. Deliberate approaches towards maintaining strong data protection policies would also speak volume about such an institution's commitment towards security and will, in turn, win trust and more extended customer relationships. People who are secured in the knowledge that their information is private are therefore more inclined to avail themselves of banking and even insurance services provided online, hence boosting the sector[326].

Data protection requirements as prescribed by the regulatory bodies in different countries have become quite stringent. Thus, data protection across the board has developed into a regulatory requirement that financial institutions must respond to by putting in place elaborate security architecture in their institutions. Organizations have to comply with laws such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and India's proposed Personal Data Protection Bill (PDPB). Non-compliance can cost organization hefty fines and other legal actions; hence data privacy becomes a paramount objective for banks and insurance companies[327].

The introduction of the measures or mechanisms like encryption, creating strong secure authentication processes, and conducting regular security audits serve as protection against sensitive customer information for financial institutions. Education

2016) https://www.weforum.org/reports/the-future-of-financial-infrastructure

[322] See, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, art 5.

[323] *Reserve Bank of India (RBI)*, 'Master Direction on Digital Payment Security Controls' (February 2021) https://www.rbi.org.in

[324] *Basel Committee on Banking Supervision*, 'Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors' (February 2018)

[325] See Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, (W.W. Norton & Co., 2015) p. 57; also see, DLA Piper, "Global Data Breach Report 2021," https://www.dlapiper.com

[326] Lothar Determann, *Determann's Field Guide to Data Privacy Law*, (4th edn., Oxford University Press, 2022) p. 22.

[327] See General Data Protection Regulation, Regulation (EU) 2016/679; California Consumer Privacy Act, Cal. Civ. Code 1798.100; The Personal Data Protection Bill, 2019 (India); also see, K. S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

of employees and customers about cybersecurity threats stemming from phishing and malware attacks would additionally protect the security of the data. As the financial industry continues to evolve, data privacy will remain a cornerstone in this evolving world of trust, security, and compliance.

3. Regulatory Framework for Data Privacy

3.1 International Regulations

Therefore, one global regulation of extreme importance is the General Data Protection Regulation (GDPR). GDPR is applicable to organizations processing EU citizens' data and imposes on them data protection and privacy responsibilities. Data minimization, user consent, notification of a breach, and right to be forgotten are some of the fundamental tenets of GDPR. Compliance with GDPR regulations is a question of self-protection for financial institutions from unjustified fines, ensuring their integrity to customers[328].
California Consumer Privacy Act (CCPA): Being a CCPA project, privacy right in California has accelerated the establishment of international standards for data protection. It offers consumers control over their personal information, including access, deletion, and exclusion from data sales. CCPA California financial institutions will be required to implement the CCPA rules, thereby providing transparency and consumer management of their personal data[329].
Basel Committee on Banking Supervision: BCBS provides risk management standards applied to banking data security. It recommends applying cybersecurity measures and operational resilience in accordance with sound internationally accepted practices to safeguard banking data from cyber threats and unauthorized access[330].

Therefore, with an understanding of these global regulations, sufficient compliance is ensured to the financial institutions, thus minimizing their risk and developing customer confidence for the banking and insurance sectors in the digital industry[331].

3.2 Data Protection Laws in Banking and Insurance in India

The protection of customer data and cybersecurity within the financial sector of India, particularly the banking and insurance sector is governed by various laws and regulatory guidelines. The following is a comprehensive discussion of some major laws and regulations pertinent to that area:

1. Information Technology Act, 2000 (IT Act, 2000)

The Information Technology Act, 2000 is India's foremost legislation regarding cybersecurity, electronic commerce, and data protection. It gives a purposeful framework for electronic records, digital signatures, and the measures under which cyber security is being pursued[332]. Among the key provisions relevant to data protection in banking and insurance are:

- **Section 43A:** Assigns liability to companies for not protecting sensitive personal data. Reasonable commercial security practices must be employed by organizations dealing with customer financial data[333].
- **Section 72:** Prescribes penalties for unauthorized access, disclosure, or misuse of personal information obtained under official capacity[334].
- **Sections 66C & 66D:** Offer protection against identity-theft and fraud which

[328] See General Data Protection Regulation, Regulation (EU) 2016/679; also see, Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, (Springer, 2017) p. 15.
[329] See General Data Protection Regulation, Regulation (EU) 2016/679; also see, Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, (Springer, 2017) p. 15.
[330] See Basel Committee on Banking Supervision, "Principles for Operational Resilience," Bank for International Settlements (2021) https://www.bis.org
[331] World Bank Group, *Cybersecurity for Development: Final Report*, (2023) https://www.worldbank.org
[332] See The Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000.
[333] Ministry of Electronics and Information Technology, "Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011," https://www.meity.gov.in
[334] The Information Technology Act, 2000, s. 72

becomes pertinent in financial transactions[335].

- **Section 79:** Allows limited liability for intermediaries like banks and insurers so long as due diligence and security measures are taken[336].

Rules Under the IT Act: The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 mandates a set of guidelines for handling personal or sensitive data, which makes it incumbent upon the banks and insurers to enforce robust security frameworks[337].

2. Personal Data Protection Bill (PDPB) (Proposed as Digital Personal Data Protection Act, 2023)

The introduction of the **Personal Data Protection Bill (PDPB)** was the first step toward regulating the collection, processing, and storage of personal data. Now known as the Digital Personal Data Protection Act, 2023, it seeks primarily to ensure proper handling of customer data by financial institutions such as bankers and insurers[338].

Some of the key provisions include:

- Data Localization: Some critical data must be stored in India to avoid its being misused by outsiders[339].
- User Consent: Explicit consent should be obtained before any collection or processing of customer data[340].
- Right to Access and Correction: Customers are entitled to apply for access to their data and for corrections in it[341].
- Fines for Breach of Data: Non-compliance will attract heavy fines that may act as deterrent against banks and insurance companies not protecting the data[342].

Once fully implemented, the legislation will greatly affect banks and insurers and will force them to revise their data protection procedures.

3. Reserve Bank of India (RBI) Guidelines on Data Protection

The introduction of the Personal Data Protection Bill (PDPB) was the first step toward regulating the collection, processing, and storage of personal data. Now known as the Digital Personal Data Protection Act, 2023, it seeks primarily to ensure proper handling of customer data by financial institutions such as bankers and insurers[343].

Some of the key provisions include:

• **Data Localization**: Some critical data must be stored in India to avoid its being misused by outsiders[344].

• **User Consent**: Explicit consent should be obtained before any collection or processing of customer data[345].

• **Right to Access and Correction**: Customers are entitled to apply for access to their data and for corrections in it[346].

• **Fines for Breach of Data**: Non-compliance will attract heavy fines that may act as deterrent against banks and insurance companies not

[335] Prashant Mali, *Cyber Law & Cyber Crimes Simplified*, (Snow White Publications, 2nd edn., 2020) p. 89.
[336] The Information Technology Act, 2000, s. 79; also see, Shreya Singhal v. Union of India, (2015) 5 SCC
[337] See The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E), dated 11-04-2011, issued under s. 43A of the IT Act, 2000.
[338] See Digital Personal Data Protection Act, 2023, Act No. 22 of 2023; also see, Ministry of Electronics and Information Technology, "Digital Personal Data Protection Act, 2023" https://www.meity.gov.in
[339] See Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 s. 33 (regarding data localization obligations for critical personal data).
[340] See Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 s. 6 (concerning notice and consent requirements).
[341] See Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 s. 11 (rights of data principals to access and correct their personal data).
[342] See Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 s. 33(3) & s. 33(4) (concerning penalties for non-compliance); also see, *Data Protection Board of India* provisions under the Act.
[343] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), available at https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023
[344] The Digital Personal Data Protection Act, 2023, s. 10, No. 22 of 2023 (India), available at https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023
[345] The Digital Personal Data Protection Act, 2023, s. 6, No. 22 of 2023 (India), available at https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023
[346] The Digital Personal Data Protection Act, 2023, s. 12, No. 22 of 2023 (India), available at https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023

protecting the data. Once fully implemented, the legislation will greatly affect banks and insurers and will force them to revise their data protection procedures[347].

4. Insurance Regulatory and Development Authority of India (IRDAI) Guidelines

Insurance Regulatory and Development Authority of India (IRDAI) is the chief regulator of the insurance domain in India. It has issued several guidelines in data protection, cybersecurity, and privacy in the insurance domain. Such regulations protect the information of policyholders, provide a protective shield against cyber fraud, and emphasize adherence to prescribed standards of data integrity[348].

Here is an insight into certain crucial IRDAI regulations pertaining to data protection:

1. Guidelines on Information and Cyber Security for Insurers (2017)

By virtue of offering a comprehensive cybersecurity framework for insurance companies, the IRDAI Guidelines on Information and Cyber Security for Insurers(2017) are aimed at ensuring protective measures by insurance companies against sensitive customer information from cyber threats[349]. Major points include:

- **Security Policy Requirement**: An insurer must have in place a detailed Board-approved cybersecurity policy that includes data security protocols.
- **Risk-Based Security Approach:** The insurer must adopt security measures on the basis of risk assessment so as to avert data breaches and cyber-attacks.
- **Data Encryption and Access Controls:** Sensitive policyholder information, including financial and health records, should have encryption and access control.
- **Incident response and reporting**: The insurer should have a mechanism for responding to cyber-related incidents and should report any data breach or suspicion of a breach to IRDAI.

Appointment of Chief Information Security Officer (CISO): Every insurer must appoint a CISO who shall be responsible for compliance with cybersecurity measures[350].

These regulations compel insurance companies to ensure rigorous protection measures over customer data and prevent cyber fraud.

2. Data Privacy Regulations (2023)

The IRDAI Data Privacy Regulations, 2023 brings in a very structured approach to collecting, processing, and storing the policyholder's data, ensuring transparency and customer consent[351]. Constitution of the following:

Collection and Processing of Personal Data: Insurance companies must receive explicit consent from customers for collecting their data and processing it.

Purpose Limitation: The data collected by an insurer should be used solely for specific legitimate purposes, such as underwriting, claims, and risk assessment.

Right to Access and Correction: Policyholders should be able to access their data, correct it, and get explanations about its use.

Restrictions on Data Sharing: Without explicit consent, insurers should not be selling or sharing information with third parties, such as marketing firms or other financial institutions.

Data Deletion and Retention Policy: Insurers should be able to define clear data retention and deletion policies once the policy period is over or the data is no longer needed.

[347] The Digital Personal Data Protection Act, 2023, s. 33, No. 22 of 2023 (India), available at https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023

[348] Insurance Regulatory and Development Authority of India (IRDAI), *About IRDAI*, available at https://irdai.gov.in/

[349] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, Ref. No. IRDAI/IT/GDL/MISC/082/04/2017 (Apr. 7, 2017), available at https://irdai.gov.in/

[350] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, Ref. No. IRDAI/IT/GDL/MISC/082/04/2017, para 7.1 (Apr. 7, 2017), available at https://irdai.gov.in/

[351] IRDAI, *Data Privacy Regulations*, 2023, Ref. No. IRDAI/REG/DataPrivacy/2023, preamble, available at https://irdai.gov.in/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

These regulations are catalysts towards strengthening customer trust in the insurance sector by ensuring data privacy and transparency.

3. Data Localization Requirements

It is now a requirement for the IRDAI that all data localization be such that critical information related to policyholders is capped and stored entirely within Indian soil[352]. The basic essence of these requirements include:

- **Storage of Critical Data in India:** Apart from sensitive policy-related papers, insurers have to store all customers' and financial-related data on Indian servers[353].
- **Restriction in Cross-Border Transfer of Data:** There are very few and rare circumstances where data may leave India, and the insurer has to comply with very stringently regulated approvals[354].
- **Data Localization Norms of RBI**: The above provisions are also applicable in the context of data localization rules as issued by RBI relating to banking and other financial institutions.

Thus, in data localization, IRDAI would ensure that sensitive data of policyholders are kept within the everlasting sovereignty of these Indian insurance companies boosting national cybersecurity.

4. Periodic Cybersecurity Audits and Risk Assessment

To ensure the maintenance of stringent standards in data protection and cybersecurity, IRDAI made it mandatory for insurers to have in place regularly cyclical risk assessments and audits on cybersecurity[355]. The salient requirements are as follows:

- **Annual Cybersecurity Audit**: This requires insurance companies to conduct at least one independent cybersecurity audit every year and submit the report to IRDAI[356].
- **Vulnerability Assessment and Penetration Testing (VAPT)**: Insurers are required to carry out VAPT periodically to identify vulnerabilities or weaknesses and the best preventive measures to be established against cyberattacks[357].
- **Risk-based Approach to Compliance:** The Insurer is expected to bring in a risk-based approach to cybersecurity that would require more stringent levels of protection for critical systems[358].
- **Employee Training on Cybersecurity:** Train employees to identify cyber threats and work along with customers' best practices while handling data[359].

This shall always allow detection and prevention of such threats through early detection and continuous improvement concerning the cybersecurity framework in the case of insurance companies.

4. Challenges in Data Privacy and Protection

Challenging Factors in Data Protection for Banking and Insurance Sector

Banks and insurance companies normally arm themselves with voluminous and sensitive customer data. Therefore, these two industries are necessarily prime targets during cyberattacks and data breaches. Several challenges are faced, however, by financial institutions posed by regulatory frameworks and other reasons in ensuring data security and compliance. There is above a detailed description of the most important challenges.

[352] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, 2017, cl. 9, available at https://irdai.gov.in/
[353] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, 2017, cl. 9.1, available at https://irdai.gov.in/
[354] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, 2017, cl. 9.2, available at https://irdai.gov.in/
[355] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, 2017, cl. 11, available at https://irdai.gov.in/
[356] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, 2017, cl. 11.1, available at https://irdai.gov.in/
[357] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, 2017, cl. 11.2, available at https://irdai.gov.in/
[358] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, 2017, cl. 10.1, available at https://irdai.gov.in/
[359] IRDAI, *Guidelines on Information and Cyber Security for Insurers*, 2017, cl. 12, available at https://irdai.gov.in/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

4.1 Cyber Threats and Data Breaches

Financial and personal data on banks and insurance companies make these organizations very vulnerable to cyberattacks. The institutions were targeted using one's attack method from the following:

Phishing Attacks: To obtain credential information, cyber thieves will make phishing emails or websites to fool customers and employees into disclosing sensitive information.

Ransomware Attacks: Encrypted key financial data requires ransom for decryption crippling banking and insurance operations.

Data Breaches: Unauthorised entry into financial databases can lead to identify stealing, fraudulent transaction and cash loss.

Malware and Spyware: The malicious software infiltrating banking and insurance systems provides opportunities for cyber criminals to steal data or manipulate transactions.

Distributed Denial of Service (DDoS): The attackers send massive traffic into a bank's or an insurer's network making online services completely inaccessible to customers.

The Influence of Cyber Threats

- **Reduction of funds:** Cyber-fraud is perpetrated by data breach.
- **Reputational Damage:** Losses due to data breaches discourage the customers from extending their online transactional and other banking and insurance experiences to the institution.
- **Regulatory Penalties:** Non-protection of customer data attracts legal action and heavy penalties under data protection laws.

The institutions have to upgrade continuously their cyber security operations to cope with the continuously changing threats.

4.2 Regulatory Compliance in an Evolving Environment

Financial institutions have to function in an extremely regulated environment with high stakes and continuously evolving data protection laws. Some of the major regulatory issues are as under:

Complex Data Protection Laws

India is still working on its Personal Data Protection Bill (PDPB) about future measures of compliance.

Global financial institutions with operations need to comply with multiple regulations such as:

- General Data Protection Regulation (GDPR) – Europe
- California Consumer Privacy Act (CCPA) – USA
- RBI and IRDAI Data Protection Guidelines – India[360]

Conflicting Needs: Jurisdictions define different requirements for storage of data, consent, and cross-border transfer which complicates compliance issues.

Complying Expenses

The expense of operating a bank or an insurance company entails investments in advanced cybersecurity infrastructure, legal experts, and compliance teams, which raises the cost of operations.

Noncompliance may result in severe penalties or litigations and further increase financial burdens.

These would require the financial institutions to adopt a proactive compliance strategy to monitor the changes in regulation and implement standardized data protection policies.

4.3 Risks Induced by Third Parties

Outsourcing IT services, data processing, and customer support to third-party vendors have a higher risk of security compromises for most financial institutions.

[360] *The Digital Personal Data Protection Act, 2023*, Act No. 22 of 2023; *General Data Protection Regulation (EU) 2016/679*, Official Journal of the European Union, L119/1, 4 May 2016; *California Consumer Privacy Act of 2018*, Cal. Civ. Code 1798.100 et seq. (USA); *Reserve Bank of India, Master Directions on IT Framework and Cybersecurity Guidelines*, available at: https://www.rbi.org.in, *Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security for Insurers (2017)*, available at: https://www.irdai.gov.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Major Third-Party Risks

Weak Cybersecurity Practices: Vendors may not have strong cyber protection protocols making them easy targets for cybercriminals[361].

Unauthorized Access to Data: External vendors are likely to mismanage sensitive financial data, leading to its breach or misuse.

Compliance Gaps: Third-party service providers are known to not fully comply with the data protection laws, opening banks and insurers to violations[362].

Mitigating Third-Party Risks

Due: Banks and insurers need to check the cybersecurity practices of vendors before signing them up.

Contractual Protections: Service agreements should also contain provisions regarding data protection clauses, confidentiality requirements, and penalties for non-compliance.

Periodic Audit: Financial institutions must carry out periodic audits that would ensure the adherence of third-party vendors to the security and privacy standards required[363].

By enforcing strict third-party risk management policies, banks and insurers can reduce exposure to data security vulnerabilities.

4.4 Balancing Security and Customer Convenience

Indeed, cybersecurity is important, but for banks and insurers, they also need to make the life of customers easy and seamless with digital experiences. Balancing security and convenience becomes one of the core problems[364].

Dilemmas of Security and User Experience

Strong Authentication vs. Ease of Access: Although multi-factor authentication (MFA) and complicated passwords provide security, they can frustrate users[365].

Fraud Prevention vs. Speed of Transaction: Often stringent fraud detection standards may lead to delaying an online transaction, and customers might not find this convenient[366].

Privacy versus Personalization: There is a personal touch that customers expect from their banks and insurance service providers; however, data privacy is mandatory for their services while using AI-powered analytics[367].

Balancing Security:

Biometric authentication: Fingerprints, facial recognition, or voice authentication increases the security standards without the needs of complicated pipeline password systems[368].

AI-Based Fraud Detection: Advanced machine learning models quickly recognize transactions yet impact none on the experience of customers[369].

Adaptive Measures: Risk-based authentication helps build security systems according to the transactions' risk levels within your bank[370].

With the help of advanced technology within security, banks and insurers will be able to maintain the highest standard of data protection while ensuring that the digital experience is fully user-friendly.

5. Best Practices for Ensuring Data Privacy in Banking and Insurance

In the banking and insurance fields, data privacy is very important since financial institutions handle sensitive customer data which consists of personal details, financial

[361] *Reserve Bank of India, Guidelines on Managing Risks in Outsourcing of Financial Services by Banks*, RBI/2006-2007/167, DBOD.No.BP.40/21.04.158/2006-07 (Nov. 3, 2006), available at: https://www.rbi.org.in

[362] *IRDAI, Guidelines on Outsourcing of Activities by Insurance Companies*, IRDA/ADM/GDL/MISC/059/03/2011 (Mar. 31, 2011), available at: https://www.irdai.gov.in

[363] *RBI, Cyber Security Framework in Banks*, RBI/2015-16/418, DBS.CO/CSITE/BC.11/33.01.001/2015-16 (June 2, 2016), available at: https://www.rbi.org.in

[364] *PwC, Cybersecurity in Financial Services: Balancing Risk and Customer Experience*, available at: https://www.pwc.com

[365] Raghavan, S., *Two-Factor Authentication and the Usability Trade-Off in Financial Services*, 12(1) Journal of Information Security (2021).

[366] Kumar, A., *Fraud Detection and Customer Experience in Digital Banking*, 27(4) Indian Journal of Finance (2022).

[367] Mitra, R., *Personalization vs Privacy: The AI Dilemma in Indian Banking*, 45(2) Company Law Journal (2021).

[368] IRDAI Guidelines on Information and Cybersecurity of Insurers, 2023; see also RBI Master Direction on Digital Payment Security Controls, 2021.

[369] Mehta, V., *AI and Fraud Detection in Indian Financial Institutions*, 19(3) Journal of Financial Crime (2022).

[370] RBI, *Cybersecurity Framework for Banks* (2016); IRDAI, *Circular on Information and Cybersecurity Risk Mitigation Measures*, 2023.

records, and transaction histories[371]. Data protection measures need to be implemented so that sensitive customer data is not only protected but also complies with regulations. A further discussion in detail explains the practices concerning data privacy in the financial industry.

5.1 Implementing Robust Cybersecurity Measures

To defend customer data against unauthorized access, virtual attacks, and fraud, dim; financial institutions need to implement sturdy cybersecurity policies[372]. Some of the major strategies include:

End-to-End Encryption

Ensures that the information transmitted to and from customers of the financial institutions stays protected from any unauthorized access[373].

Encryption of sensitive information such as credit card details, banking credentials, and insurance policy information is accounted for.

Multi-Factor Authentication (MFA)

Provides security through verification based on more than one factor (e.g., password, biometric authentication, or OTP) before allowing access to the accounts[374].

This would prevent unauthorized access and identity theft better.

Regular Security Audits and Vulnerability Assessment

Periodic evaluation of security measures will help sort the weaknesses of the banking and insurance systems[375].

Penetration testing would ensure that any possible threats from within the cyberworld would be identified and put off before actual damage is incurred.

By employing these measures, banks and insurance firms can diminish their cyber risks, thus growing customer trust[376].

5.2 Data Minimization and Secure Storage

In fact, collecting and storing only necessary data reduces security exposure and increases compliance with data protection regulations[377].

Data Minimization

This is essential customer account information for transactions and regulatory compliance that banks and insurers should acquire from a customer[378].

Unnecessary data collections always minimize the potential risk of a resident's privacy breach in a data breach.

Keeping Data Secure

It needs to be entered into high-level encryptions to make sure it remains unreadable after being stolen.

Tokenization and anonymization are other techniques for securing stored data.

Access Controls and User Authentication

This should involve collections access control to restrict sensitive information access only to authorized personnel[379].

Access Management Based on Roles (RBAC): This enables limiting data access according to the job roles of employees[380].

Financial institutions can then reduce the chances of data leaking and ensure customer privacy by following these practices of data minimization and secure storage.

---

[371] Sharma, R., *Data Protection in the Indian Banking Sector: Challenges and Developments*, 55(2) Indian Bar Review 124 (2021).
[372] Sharma, P., *Cybersecurity and the Indian Financial Sector: Evolving Challenges and the Legal Framework*, 62(3) Journal of Indian Law Institute 245 (2020).
[373] Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, RBI/DoS/2021-22/63, dated 18-02-2022.
[374] Insurance Regulatory and Development Authority of India (IRDAI), *Guidelines on Information and Cyber Security for Insurers*, IRDAI/IT/GDL/MISC/081/04/2023, dated 24-04-2023.
[375] Ministry of Electronics and Information Technology (MeitY), *National Cyber Security Policy*, 2013
[376] Kumar, R., *The Legal Dimensions of Cybersecurity in the Financial Sector*, 48(1) Indian Bar Review 137 (2022).
[377] Sharma, P., *Data Privacy and Security in the Financial Sector: Legal and Operational Aspects*, 61(2) Journal of Indian Law Institute 178 (2019).
[378] Reserve Bank of India, *Master Direction on Information Technology Framework for NBFCs*, RBI/DNBR/2017-18/42, dated 08-06-2017.
[379][379]
[380] Kumar, R., *Cybersecurity Practices in the Indian Financial Services Industry: Emerging Trends*, 49(3) Indian Bar Review 210 (2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

5.3 Compliance with Regulatory Requirements

- Data protection regulation given by national or international authorities must be complied with by banks and insurers to preempt the possibility of legal penalties and to protect customer data[381].
- Employees must receive training on data privacy laws such as the Information Technology Act, the RBI guidelines, the IRDAI regulations, and the pending Personal Data Protection Bill (PDPB)[382].
- Training is to be given in best practices for cybersecurity, prevention of phishing attacks, and data handling procedures.

Establishment of a Compliance Management System

- The compliance management system (CMS) assists financial institutions with monitoring the regulatory changes as they occur and implementing them effectively[383].
- CMS provides that internal policies and procedures not only define the organization's goals in moral or ethical terms but also assure and attest compliance with legal and regulatory requirements[384].
- In quick accession to all regulatory requirements, banks and insurers can come forth and absolutely limit their data privacy violation risks through this[385].

5.4 Strengthening Consumer Awareness

Those can best be thought as educating customers on how to protect their strong financial data and malicious cyber threats.

A cyber security awareness campaign:

It should be challenged by banks and insurers to the public with awareness events on:

- Scams through phishing, by email and by phone.
- Strong password use and safe online banking.
- Online banking financial transactions using public wi-fi.
- Secure Communication Channels for Transactions
- All customer banking should occur over encrypted and authenticated communication channels.
- Encouragement of the official mobile banking apps and secure web portals is to prevent fraud.

Apart from increasing awareness among consumers, financial institutions might keep consumer confidence up and cut down cyber fraud threats.

5.5 Enhancing Third-Party Risk Management

Most banks and insurance companies rely on third parties to provide payment processing, IT services, and data storage. However, these outside services complicate security requirements that they have to manage.

Thorough Investigations and Normal Audits

Financial companies should investigate well into agreements with outside parties[386].

Normal examinations and cybersecurity assessments must then be enforced against every vendor to see if their practices comply with parameters set by data protection laws[387].

Data Protection Obligatory in the Contracts for Service Providers

Contracts with outside vendors should Include such:

- Information security clauses demanding strict confidentiality of customer data.

[381] Sharma, V., *Compliance and Data Privacy in Financial Services under Indian Law*, 62(1) Journal of Indian Law Institute 134 (2020).
[382] Ministry of Electronics and Information Technology, *The Digital Personal Data Protection Act, 2023*, Act No. 22 of 2023
[383] Sengupta, R., *The Role of Compliance Management Systems in the Indian Banking Sector*, 59(2) Journal of Indian Law Institute 204 (2017).
[384] Reserve Bank of India, *Master Direction – Information Technology Framework for the NBFC Sector*, RBI/DNBR/2016-17/45, dated 08-06-2017.
[385] Kapoor, M., *Legal Risk Management and Compliance Systems in Financial Institutions*, 65(3) Indian Bar Review 311 (2022).
[386] Sharma, A., *Vendor Risk Management in Financial Institutions: A Legal Approach*, 64(4) Indian Bar Review 567 (2021).
[387] Reserve Bank of India, *Guidelines on Outsourcing of Financial Services by Banks*, RBI/2006-2007/283, dated 03-11-2006.

- Compliance specifications associated with the requirements of the RBI and IRDAI.
- Penalties for breach of data and non-compliance[388].

Banks and insurers can improve third-party risk management and therefore make sure high data security standards are met by external providers[389].

6. Conclusion

In the contemporary digital age, data privacy and protection are critical considerations in the banking and insurance industries because of the sensitivities they are expected to handle in customer information. Increasingly rampant cyber threats, including phishing attacks, ransomware attacks, and unauthorized access, have made it increasingly important that financial institutions care for their customers' data with robust security. Regulatory authorities like the Reserve Bank of India (RBI) and the Insurance Regulatory and Development Authority of India (IRDAI) have laid out stringent guidelines to ensure compliance with the data protection standards. Financial institutions ought to implement strong cybersecurity infrastructures encapsulating encryption, multifactor authentication, and regular audits to mitigate risks and avoid financial fraud. Consumer awareness regarding cybersecurity threats and safe digital banking practices must also be promoted to enhance data protection. By promoting data security, regulatory compliance, and consumer education, commercial banks and insurance companies can contribute to a secure digital ecosystem with trust, financial stability, and security of sensitive information in the ever-growing trend of digitalization.

[388] Insurance Regulatory and Development Authority of India (IRDAI), *Guidelines on Outsourcing of Activities by Insurance Companies*, IRDA/ADM/GDL/GLD/074/04/2017, dated 20-04-2017.
[389] Kapoor, R., *Strengthening Third-Party Risk Compliance in the Digital Age*, 60(1) Journal of Indian Law Institute 92 (2018).