Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Data Protection in the Digital Age: Indian Banking Sector's Cyber Security Imperative

Article History:

Name of Author:
Dr. Sonal Rawal[1], Dr. Ishani Dave[2], Dr. Vaishakhi Thaker[3], Dr. Aditi Jani[4] and Dr. Hiral Shukla[5]

Affiliation:
[1]Assistant Professor (Law), Faculty of Law, GLS University, Ahmedabad
[2]Assistant Professor (Law), Faculty of Law, GLS University, Ahmedabad
[3]Assistant Professor (Law), Faculty of Law, GLS University, Ahmedabad
[4]Assistant Professor (Law), Faculty of Law, GLS University, Ahmedabad
[5]Assistant Professor (Law), Faculty of Law, GLS University, Ahmedabad.

Corresponding Author:
Dr. Sonal Rawal

Email: *reenkuraj539@gmail.com*

How to cite this article: Rawal S, *et al.* Data protection in the digital age: Indian banking sector's cyber security imperative. *J Int Commer Law Technol.* 2025;6(1):60–67.

Received: *12-07-2025*
Revised: *29-07-2025*
Accepted: *18-08-2025*
Published: *30-08-2025*

Abstract: The rapid advancement of technology has transformed the Indian banking sector, leading to the emergence of online and digital banking services such as mobile banking, e-payments, and virtual cards. Innovations including Artificial Intelligence, blockchain, and robotics have further enhanced efficiency and convenience in financial services. However, these developments have also heightened vulnerabilities associated with large-scale data collection and exchange, exposing the sector to significant cyber security threats. Ensuring privacy and data protection has thus become a critical concern, as customers entrust banks with sensitive personal and financial information, creating an obligation of confidentiality. Global incidents, such as the Cambridge Analytica scandal, highlight the potential misuse of data and reinforce the urgency of strong safeguards. Within the Indian context, the issue assumes particular importance due to the increasing digitalization of financial systems and growing reliance on customer data. This paper examines the existing legislative and regulatory framework for cyber security and data protection in the Indian banking sector, analyzing the duties of confidentiality imposed on banks and the adequacy of current mechanisms. It argues that while cyber security is essential to protect data, robust data protection norms are equally necessary to preserve privacy, ensure customer trust, and secure the integrity of the banking system.

Keywords: Cyber Security, Data Protection, Indian Banking Sector, Privacy, Confidentiality, Digital Banking.

INTRODUCTION

One of the most crucial breakthroughs of the modern era has undoubtedly been thetechnology and its advancement. The advancement of technology has brought great strides in every sector and no facet of human life has been left uninfluenced. Consequently, banking sector has not been left out of its breakaway. Online Bankingand Digital Banking are both by products of this intervention of technology in the banking sector. Over the last few years, the bankingindustryin India has feltthe need tokeep upwiththeglobalbankingstandardswhich led to banks upgrading their technology and services. More investment was channeled towards creation of digital infrastructure to provide services like mobile banking, e-payment services, virtual cards etc. Artificial Intelligence, Robotics, Block Chain Technology and Bit coin are some of the crucial innovations in Digital Banking. These services are possible because of communication and exchange of data at very large scale, of data belonging to customers. The collection and exchange of data is a

highly vulnerable mechanism owing to all cyber security threats associated with it.

Privacyhas been focusing point offew ofaheateddebatesin therecent years. Thedigital erahas just added to theseconcerns relatingto privacy. The lives of people arestored in form of data, crossing borders and existing out there in a virtual space making it vulnerable tomanipulation. The best case in point would be the Cambridge Analytica scandal which just goes on to prove how much data in the virtual space can be exploited. A person should have complete ownership over his information. The concept of privacy is based on this ownership over his information and trust certainly plays an important role in this. Privacy plays an essential role in banking sector. A person approaching a bank, places his trust in the same bank by giving his information, creating an obligation on the banks to not divulge that information.

Information security and privacy are some of the alarming threats facing the banking industry currently. These threats not restricted to Indian Banking industry per se but also extend to Banking industry at global level. The aim of this article is to discuss in context of India the existing mechanism and framework for "Data Protection and Cyber Security" in the Indian Banking sector. The article starts with Cyber Security and current legislative framework in that regard. Subsequently, it discusses the laws which require data protection and duty of confidentiality. Data Protectionand Cyber Security are quite related in these nsethatlatteris necessary so that data is protected and does not go in unauthorized hand smakingitvulner able to manipulation.

CYBER CRIMEAND CYBER SECURITY: OVERVIEWAND BACKGROUND

The Indian banking industry is enjoying a joyous growth. With the credit card and debit card users increasing every day and new technologies like internet wallets slowly gaining popularity, the financial transaction saretouching all-time highs. To provide improved support for cashless transactions, a steady increase in the number ATM and POS machines is inevitable.

Former RBI governor, Raghuram Rajan, had announced that the central banking institution is in the process of setting up an Information Technology (IT) subsidiary to aid the RBI in effectively monitoring and supervising internet-based services offered by banks across the country.This is a welcome move for the Indian banking sector and its customers who are threatened by systemic vulnerabilities, which enable technology related banking and financial frauds,1 birthed primarily by the continued migration of services to internet and mobile platforms.

With increasing risks of cyber threats, banks are facing an extraordinary challenge of data breaches and are therefore strengthening their cyber security postures. The following are the noticeable trends in banking industry from cyber security point of view:

- Financial sector faced almost three times the cyberattacks as compared to those of other industries;
- Databreaches(bothinternal throughfraudandexternal throughcybercriminals)leads to the exponential rise in costs;
- It has been estimated that cost of implementing and managing the cyber security infrastructure will increase over 40% by 2025;
- There is an increase in biometrics and tokenization as banks have begun to recognize that in addition to being a solution for payments, these controls are also useful in securing the sensitive data;
- Customers are using biometrics for banking activities such as authentication formobile banking, transaction at ATMs and payments;
- With digital channels becoming the preference choice of customers for banking services, banks will also need to leverage advanced authentication and access control processes, without any compromise to customer experience.

There is a visible shift in the banking industry in the way customers deal with their transactions and a rapid increase in the usage of digital channels such as internet banking, digital wallets, mobile banking, ATM leading to the increase in exposure and thereby cyberattacks which further may lead to financial and reputational losses. Banks may lose customer confidence which can further increase the impact.

The key influencers which make it authoritative for the banks to invest in security are:

- Increase in financial data losses including card data, personal identifiable information etc.
- Unauthorizedaccesstobank'snetworkan d systems.

As an increasing number of users are demanding online services, the background mission of providing balanced security and convenience appears to be a tough challenge due tonumerous conspicuous actors collectively referred to as "Cyber-Crime". Cyber-Crime isbeing considered a serious threat to all the aspects of a nation's economic growth asmaximum instances of the same are being observed in financial institutions. Cyber-Crime incidents include credit card fraud, spamming, spoofing, e-money laundering,

ATM fraud, phishing, vishing, identity theft and denial of service.

In other words, Cyber Crime can be simply stated as crimes that involve the use of computer and a network2 as a medium, source, instrument, target, or place of a crime. With the growing aspect of e-commerce and e-transactions, the economic crime has shown a shift towards the digital world. Cybercrimes are increasing globally and India too has been witnessing a sharp increase in cybercrimes related cases in the recent years.

Believed to be India's first legal adjudication of a dispute raised by a victim of a cybercrime in phishing case, the adjudicating officer at Chennai, Govt. of Tamil Nadu directed ICICI Bank to payRs 12.85 lakhs to an Abu Dhabi-based non-resident Indian within 60 days forthe loss suffered by him due to a phishing fraud. Phishing is a form of internet fraud through which sensitive information such as usernames, passwords, and credit card details isobtained by masquerading as a trustworthy entity.

The ruling was passed under the Cyber Regulations Appellate Tribunal Rules, 2000, with Tamil Nadu IT secretary PWC Davidar acting as the adjudicator under the Information TechnologyAct, 2000. The application was filed before Adjudication Officer for the State for adjudication under Section 43 read with section 46 of the Information Technology Act, 2000. Sivasubramanian, an NRI employed in Abu Dhabi, maintained a bank account with ICICI Bank and had Internet banking access for his savings bank account. In September 2007, he received an email from the bank asking him to reply with his internet banking username and password or else his account would become non-existent. Assumingit to be a routine mail, he complied with the request. But later, he found that Rs 6.46 lakh were transferred from his account to one Uday Enterprises, an account holder in the same bank in Mumbai, which withdrew Rs 4.6 lakh by self cheque from an ICICI branch in Mumbai and retained the balance in its account. When ICICI Bank tried to contact the firm, it found that Uday Enterprises had moved on from the address it had provided two years earlier.

Sivasubramanian contended that the bank had violated the "know your customer" (KYC) norms, filed a criminal complaint and also appealed to the State Government's IT Secretary, Mr. P.W.C. Davidar, the Adjudicating Officer under the IT Act. The bank claimed that Sivasubramanian had negligently disclosed his confidential information, such as hispassword, and as a result became a victim of phishing fraud.

Mr. Davidar stated in his order that a list of instructions the bank had put up on its Web site and which it sends to customers were of a "routine nature" and did not help a customer distinguish between an e-mail from the bank and an e-mail sent by a fraudster. He observed that the bank had not provided additional layers of safeguard such as due diligence, KYC norms, and automatic SMS alerts and rejected the bank's effort to take shelter behind routine instructions on phishing stating that the bank failed to take steps to prevent unauthorized access to its customers' accounts. The judgment, is significant as it is apparently the first verdict in a case filed under the IT Act awarding damages in a phishing case.

THE PROBLEM AND CHALLENGE

Today, web technology has emerged as an integral and crucial part of the Indian Banking sector because the enlargement of non-cash-based transactions around the globe has resultedin the steady development of online payment systems.

Currently, phishing, vishing, spyware or malware attacks, key logging, data theft and other internet-based frauds have been reported to be the most common cyber-attacks against banks anditscustomers.4Despitethesethreats, thereremainscontinuedandevenmorerapiduse ofinnovative, technology-backed financial servicessuch as mobile banking and social media payment systems.

India has seen a rise in the volume of debit/credit cards due to increased online acceptance through alternative channels, including internet, ATM and mobile banking. While theadoption of IT for banking services offers unprecedented convenience, cost-effectiveness, and speed of delivery, it is riddled with several external threats and suffers from lack of coordination.5

With the significant risks of adopting information technology in the delivery of banking services, a significant rise in banking-related technology frauds has been reportedand is a cause for concern for customers, commercial banks and the RBI. Major commercial banks have also been accused of not filing reports of suspicious transactions, an obligatory requirement when there has been an instanceofunsatisfactoryidentification, which allowsfor speculation that more fraudulent transactions are attempted than are reported.

The banking industry has recognized the risks associated with the penetration of IT into financial services; the proposed IT subsidiary of RBI could prove to be a great institutional addition. The threat highlighted above, demonstrates the need for a dedicated IT subsidiaryto evaluate technical capabilities of banks and provide support in beefing up cyber security inthe sector. As the exact form and mandate for the IT arm of the RBIhas not been set yet, it can also be designed to act as an information sharing resourcesimilar to the dedicated cellthatwastobeformedundertheguidanceofInstitutefor DevelopmentandResearchin Banking Technology (IDRBT)6and work towards ensuring compliance of commercialbanks to RBI notifications, codes and rules pertaining to cyber

security and data protection. Since banking, a finance sector function, potentially falls in the category of critical information infrastructure,7there needs to be constant security vigilance and cyber security measures on par with global standards.

In addition to exploring methods in which the possibilities of IT can be harnessed for effective, cost-efficient, real-time delivery of banking services, it is also crucial for this proposed subsidiary to concentrate on evolving binding basic standards of data security, privacy which is currently, primarily driven by Information Technology Amendment Act, 2008 in thebankingsector.8Thesubsidiarywhich currentlyaims to track evolvingthreats and vulnerabilities should also attempt developing real-time fraud prevention models and increase customer confidence by increasing effectiveness of independent financial IT controls. Few of the major challenges faced by banks include:

- Strict compliance regulations: Managing regulatory compliances has become extremelychallengingfor the banks. Alongwith the larger banks, smaller ones too are required to fulfil the regulatory obligations.
- The struggle to secure customer data: There are number of ways in which violation of privacy can take place in banking sector like stolen or loss card data, unauthorized sharing of data with third parties and loss of client's personal data due to improper security measures.
- Third party risk: Banks need to conduct due diligence on third parties they are associatedwith. Thirdparties need to reportanycritical issues associatedthecarddata environment to the bank.
- Evolving cyber threat landscape: The development in technologies is leading to the latest cyber threats like next generation ransom wares, web attacks etc.
- Transaction frauds: Fraud detection technologies should be in place with proper consideration of risks based on the business factors.

REGULATORY PERSPECTIVE: RBI' S ROLE

The RBI, which is the central banking institution of the country is responsible for the supervision and regulation of the finance sector, and bears the onus of evolving and enforcing parameters of banking operations. Considering the certainty of increaseddigitization of traditional banking services and accompanying vulnerabilities, the RBI has previously attempted to address the issue of cyber security by evolving minimum standard cybersafetynormsforbanksandotherprovidersoffinancialservices. In2010, theRBIsetup a working group to examine issues arising out of IT penetration and use in the banking sector and directed banks to appoint aChief Information Security Officer (CIO) and a committeeon information security. Based on the report, it also issued aset of guidelineson information security, technology risk management and combating cyber fraud, in 2011. Some of the key features of the regulations are:

- Cyber Security Policy to be distinct from the broader IT policy / IS Security Policy of a bank
- Arrangementforcontinuoussurveillance
- Comprehensivenetworkanddatabase security
- Protectionofcustomerinformation
- Cybersecuritypreparedness indicators
- CyberCrisisManagementPlan
- ITarchitectureshouldbe conducivetosecurity
- Animmediateassessmentofgapsinpreparednesstobereportedto RBI
- Cybersecurityawarenessamongstakeholders/TopManagement/Board

The guidelines provided detailed insight into building fraud risk perspective in banks, customizing audits to detect irregularities and vulnerabilities and even the appropriate reporting of fraud cases to law enforcement and other relevant stakeholders.9Even though the guidelines dealt only with issues of data security and privacy, the IDRBT, the IT institute set up bythe RBI, released a handbook on information securitygovernanceto thebankingsector, to act as a follow-up to the above-mentioned guidelines.

Unfortunately, the se guide lines which were considered minimumbeststandardsand criticized to be implemented in a phased manner10, have not been taken seriously and severalbankshave failed to implement these guidelinesand carry out required cyber due diligence. The same year, RBI also released the Information Technology Vision Document 2011-2017that highlighted its recognition of the enormity of the threat that is cyber-attacks and reiterated its commitment to mitigating IT fraud in the banking sector. In 2013, it also issued a circularon risk mitigations measures to be undertaken during e-payment transactions to help bankssecure electronic payment transactions such as RTGS, NEFT and IMPS from cyber-attacks. Noting the significant increase in fraud in online banking transactions, RBI also advisedbanks to introduce two or three-stage authentication and transaction verification.11

Security Considerations

Whileeachbankthinksdistinctively onadoptingvariousconsiderations,itisimperativeto

assume that the theme remains the same for various banking channels:
Internet Banking: Security control slike multi factor a uthentication, creation of strong passwords, adaptive authentication, image authentication, etc. can be considered.
Mobile Banking: It should be ensured that mobile applications are up to date and should betested. Latest standards could be implemented.
Wallet Transactions: Awareness material on Phishing, Malware attacks, vishing and social engineering, Password security etc. should be incorporated.
ATM Security: Biometric slikeeye- retina, voices canorfingerprintscanshouldbe introduced by Banks.
Banks must conduct regular drills, awareness programs and simulation exercises to keep their infrastructure secured.

Safe guarding the Internet Banking Sector:Conclusion
Financial organizations in today's date requires well laid cyber security teams with distinguished digital leaders. Many organizations still are leaving first response to their IT teams without adequate intervention or support from senior management and other key players. employed to take a proactive stand when it comes to cyber security and privacy.Organizations in the BFSI sector need to undergo rigorous and continuous cybercrime risk assessments to precisely assess, identify and improve their present security posture byviewingtheorganization'spoliciesfromanattacker's perspectiveandthusfacilitateenhanced security, operations, organizational management. A comprehensive threat intelligence technology is essential to raise organized and analyzed threat information about potential or currentattacksfromtheorganization'sperspectiveand ithelpsorganizationsinunderstanding the common threat actors including latest vulnerabilities, exploits and advanced persistent threats campaigns.
Indian customers are graduallypreferringonline services because of convenience, cost-saving, and swiftness of online transactions. Financial institutions are throwing exciting offers to customers with the vision of overturning the volume of cashless transactions due to comparatively lower operational costs. Notably financial gain is still one of the major motivations behind most cybercriminal activities and there is little chance of this changing in thenearfuture. However, it can beconcludedthat cybersecuritymeasures placed byfinancial institutions to curtail the curse of cybercrime are being out- paced by dynamic technological landscape and improved expertise of the intruders. Non-existent/Inadequate awareness campaigns simplify the work of the cyber criminals. Traditional law enforcement policies, standards and methods have been proved insufficient to cater to the evolving cybercrimes and the IT Act of India has been marked down time and again.

LEGAL FRAMEWORK FOR DATA PROTECTIONIN BANKING SECTOR

***Laws Specificto Banking Sector-**

Section 45E of Reserve Bank of India Act, 1934: Disclosure of information prohibited - (1) Any credit information contained in any statement submitted by a banking company under section 45C or furnished by the Bank to any banking company under section 45D, shall be treated as confidential and shall not, except for the purposes of this Chapter, be published or otherwise disclosed.
Section 44 of State Bank of India Act, 1955: Obligation as to fidelity and secrecy - (1) The State Bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating toortotheaffairsofitsconstituentsexceptincircumstances inwhichitis, inaccordancewith thelaworpracticeandusagecustomaryamongbankers, necessaryorappropriatefortheState Bank to divulge such information.
Section 52 of The State Bank Of India (Subsidiary Banks) Act, 1959: Obligation as to fidelity and secrecy - (1) A subsidiary bank shall observe, except as otherwise required bylaw, the practices and usages customary among bankers, and in particular, it shall not divulge any information relating to, or to the affairs of, its constituents except in circumstances in which it is, in accordance with the law or practice and usage customary.
Section 13 of the Banking Companies (Acquisition and Transfer of Undertakings) Act, 1980: Obligations as to fidelity and secrecy - (1) Every corresponding now bank shallobserve, except as otherwise required by law, the practices and usages customary among bankers, and in particular, it shall not divulge any information relating to or to the affairs ofits constituents except incircumstances in which it is, inaccordance with law or practices and usages customaryamong bankers, necessaryor appropriate forthe correspondingnew bank to divulge such information.
Section 3 of Public Financial Institutions (Obligations as to Secrecy and Fidelity) Act, 1983:Obligation as to fidelityand secrecy- (1) Apublicfinancial institution shall not, except as otherwise provided in sub-section (2) or in any other law for the time being in force, divulge any information relating to, or to the affairs of, its constituents except incircumstances in which it is, in accordance with the law or practice and usage, customary among bankers, necessary or appropriate for the public financial institution to divulge such information.

Section 22 of The Payment and Settlement Systems Act, 2007: Duty to keep documents in thepayment system confidential -(1)Asystem providershall not discloseto anyotherperson theexistenceorcontentsofanydocument orparttherеoforotherinformation givento him by a system participant, except wheresuch disclosure is required under the provisions of this Act or the disclosure is made with the express or implied consent of the system participant concerned or where such disclosure is in obedience to the orders passed by a court of competentjurisdiction or astatutoryauthorityinexercise ofthe powersconferred bya statute.

RBI's "Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card Operations of Banks." (2013) 12

It gives provision for Right to Privacy and Customer Confidentiality and is applicable on the credit, debit and pre-paid card issuing banks and credit card issuing NBFCs, who should adhere to these guidelines strictly.

Paragraph No. 6.2states that the card issuing bank/NBFC should not reveal any information relating to customers obtained at the time of opening the account or issuing the credit card to any other person or organization without obtaining their specific consent, as regards the purpose/s for which the information will be used and the organizations with whom the information will be shared.

Paragraph No. 25titled "Customer Confidentiality Obligations" provides for Banks obligation to secrecy under the customary banking law. It also prohibits collection of information from users for cross-selling purposes.

Paragraph No. 8.1provides that information Security is most critical to the business of mobile banking services and its underlying operations. Therefore, technology used for mobile banking must be secure and should ensure confidentiality, integrity, authenticity, and non- reputability.

RBI'sNotificationon"CyberSecurityFrameworkinBanks"

Paragraph No.10states that banks depend on technology very heavily not only in their smooth functioning but also in providing cutting-edge digital products to their consumers and in the process collect various personal and sensitive information. Banks, as owners of such data,shouldtakeappropriatestepsinpreservingtheConfidentiality, IntegrityandAvailability of the same, irrespective of whether the data is stored/in transit within themselves or with customers or with the third party vendors; the confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be put in place by banks.

Section 29 of Credit Information Companies (Regulation) Act, 2005: Obligations as to fidelity and secrecy. - (1) Every credit information company shall observe, except as companiesanditshallnotdivulgeanyinformation relatingto,ortotheaffairsof,itsmembers or specified users.

The Chapter VI of this Act provides for "Information Privacy Principles and Furnishing of Credit Information."Section 19: Accuracy and security of credit information.—A credit information company or credit institution or specified user, as the case may be, in possession or control of credit information, shall take such steps (including security safeguards) as may be prescribed, to ensure that the data relating to the credit information maintained by them is accurate, complete, duly protected against any loss or unauthorized access or use or unauthorized disclosure thereof.

Section 22 prohibits unauthorized access to credit information and prescribes punishment for that same.

RBIalongwith Indian Banks Association set up BankingCodes and StandardsBoardof India to develop a comprehensive code for fair treatment of customers by banks.15 Code of Banks Commitment to Customers was brought by this board which discusses provisions on privacy and confidentiality under Paragraph 5. This code is followed by most banks in India.

General Laws for Data Protection

Apart from laws specifically relating to banking sector, Information Technology Act, 2000 also provides for Data Protection. In 2008, Section 43A and 72A of the Information Technology Act, 2000 (IT Act) were introduced by way of an amendment, to advance the cause of data privacy and protection.

Section43A ofInformationTechnologyAct, 2000: Compensationforfailuretoprotectdata

-Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Section 72A of Information Technology Act, 2000: Punishment for disclosure of information in breach of lawful contract - Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing servicesunderthetermsoflawfulcontract, hassecuredaccesstoanymaterialcontaining

personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the

consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

Additionally, in 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules or the Rules) were brought to create a more vigorous system for protection of Sensitive Personal Data or Information (SPDI). Among various kinds of information which constitute SPDI(and are hence protected under the SPDI Rules), is financial information such as bank account details, credit card or debit card or other payment instrument details, information relating to passwords, credit/ debit cards information, biometric information (such as DNA, fingerprints, voice patterns, etc. that are used for authentication purposes), physical, physiological and mental health condition, etc. SPDI Rules also lay down the security practices and procedures which banks, in possession of SPDI must follow.

Rule 4provides that the body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information,shall provide a privacypolicyforhandlingofordealinginpersonalinformation includingsensitive personal data or information.

Rule 5provides the guidelines that need to be followed by a BodyCorporate while collecting information.

Rule 8provides the reasonable security processes and procedures that may be implementedby Body Corporates. Additionally, an audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant upgradation of its process and computer resource.

Enforcement

Despite of these regulations, laws and notifications being in place, there are still cases of breach of data protection or data privacy because of shortcomings in enforcement mechanism of these laws. This is can be seen through cases where banks have been held liable for such breachofdataprotection. InonesuchcaseofPunjabNationalBankv.RupaMahajan Pahwa16, husband and wife had a joint savings account which was to be operated byeither or the survivor. Subsequently they filed for divorce. During the court proceedings husband produced the duplicate passbook of her account and used against her. On inquiry, it was revealed that the bank gave passbook to third party at the instance of the husband. She filed a complaint against the bank in District Consumer Forum stating that production of duplicate passbook led to revelation of her confidential details which would drastically affect the amount of maintenance and alimony. The bank was held liable for giving information to third party.

RECENT DEVELOPMENTS

Recently RBI came up with a notification in April 2018 which makes it mandatory for all payment service providers including payment banks and payment gateways to store payment system data in India.17 This move in the direction of Data Localization can be considered an attempt bythe RBI to have unfettered supervisoryaccess over data keeping in view the global concerns on data security and data sovereignty. However, it has faced quite a backlash from payment system providers since they would have to set up infrastructure for local storage of data.

GlobalScenario

India is far behind in terms of Data Protection Laws when compared with other countries. Recently European Union came up with General Data Protection Regulation (GDPR) which came into force in May, 2018. This framework has made data protection regime of European Union as one of the most developed data protection mechanisms in the world. Under this framework data can be collected only legally and for legitimate purposes (Article 5(1)(b)). Anyviolation of data privacy would have to be informed bydata controller to the supervisory authority within 72 hours (Article 33). It also provides for processing of data, legalobligations and accountability of entity collecting data and right to access and erasure of data subject to the data. Violation of provisions can lead to fine of 20 million Euros or 4% of the total worldwide annual turnover of the preceding financial year (Article 83).

GDPR and Banking Sector: GDPR like any other data protection law would have great impact on banks. Banks as entities have to deal with huge quantities of data. Theycollect and process data of their customers on a large scale. They are also susceptible to data thefts and cyber-attacks. In the view of these it would be necessary for banks to upgrade their existing mechanism of defenses to inculcate regulatory provisions given in the GDPR. IT system inthe banks would have to be redesigned to endure best data protection mechanisms. Reporting ofthebreaches would be mademandatory(Article33). DataProtection Officerwould haveto be appointed (Article 37). Thus, GDPR creates necessity for banks to revamp their structures in the light of concerns for data protection and security.

United States, though does not have a comprehensive law on Data Protection, has sector specific or industry specific or medium specific data security laws and states have their own laws. Thus, residents have dual protection of both state law and national law. Apart from this even Asian Countries like South Korea and

Singapore have laws in place for Data Protection.SouthKoreahasPersonal Information ProtectionAct,2011whichwasmademore stringent in 2016 to provide for stricter penal provisions for violation. On the other hand, Singapore is governed by Personal Data Protection Act, 2012. In comparison to these countries, India lags in terms of comprehensive law for data protection.

CONCLUSION VIS-À- VIS PERSONAL DATA PROTECTION BILL,2019.

A Data Protection Law was long due in India and discussions to introduce one were in place since long. Justice Srikrishna Committee came up with much awaited draft Personal Data Protection Bill in July, 2018. However, the bill has not received desired reception within the legal community.

Thereafter, the Personal Data Protection Bill, 2019 ("PDPB")was introduced in Lok Sabha by the Minister of Electronics and Information Technology, on December 11, 2019. The purpose of this Bill is to provide for protection of privacy of individuals relating to their Personal Data and to establish a Data Protection Authority of India for the said purposes and the matters concerning the personal data of an individual. The Bill proposes to supersede the Information Technology Act, 2000 (Section 43-A) deleting the provisions related to compensation payable by companies for failure to protect personal data. The PDPB inter alia, prescribes the way personal data is to be collected, processed, used, disclosed, stored and transferred18.

The PDPB proposes to protect "Personal Data"relating to the identity, characteristics trait, attribute of a natural person and "Sensitive Personal Data such as financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political beliefs.

Data protection requires more stringent law in force and better enforcement mechanism. Data Localization would not make much difference to it until enforcement mechanism improves. Thus, it can be concluded reasonably that the core problem even about regulations of data protection for banks is of enforcement, as can be seen from cases of violation of data protection. Banks should keep themselves updated about the status of the bill since it would have huge impact on how banks deal with data of the customers and would have to revamp their infrastructure to bring it in line with the law. It can be considered as a positive start for data protection regime though there is a long way to go.

REFERENCES

1. Reserve Bank of India plans IT arm, to hire experts to work on banking technologies [Internet]. The Economic Times; 2015 Oct 26 [cited 2025 Aug 29]. Available from: http://economictimes.indiatimes.com/industry/banking/finance/banking/reserve-bank-of-india-plans-it-arm-to-hire-experts-to-work-on-banking-technologies/articleshow/49512043.cms
2. Kharouni L. Automating online banking fraud: Automatic Transfer System – the latest cybercrime toolkit feature [Internet]. 2012 [cited 2025 Aug 29]. Available from: https://www.symantec.com/
3. Umashankar Sivasubramanian v. Branch Manager, ICICI Bank and others, Petition No. 2462/2008 (Decided Apr 18, 2010).
4. RBI asks banks to set up committees to protect IT data [Internet]. The Economic Times; 2011 Apr 30 [cited 2025 Aug 29]. Available from: http://articles.economictimes.indiatimes.com/2011-04-30/news/29490905_1_banking-and-mobile-banking-electronic-channels-frauds
5. Banks bet big on technology to boost efficiency, curb fraud [Internet]. Mint; 2011 [cited 2025 Aug 29]. Available from: http://www.livemint.com/Industry/8df71WBdwALasI5afwadUJ/Banks-bet-big-on-technology-to-boost-efficiency-curb-fraud.html
6. Institute for Development and Research in Banking Technology. An initiative for research and intelligence gathering related to security incidents in financial services sector for analysis & sharing of insight [Internet]. 2012 [cited 2025 Aug 29]. Available from: http://www.idrbt.ac.in/PDFs/PT%20Reports/2012/RekhaAG_AnInitiative_2012.pdf
7. Department of Electronics and Information Technology (DeitY), Government of India. Cyber Security Strategy – Strategic Approach [Internet]. 2015 [cited 2025 Aug 29]. Available from: http://deity.gov.in/content/strategic-approach
8. PSA Legal. Risk management in e-banking [Internet]. 2009 [cited 2025 Aug 29]. Available from: http://psalegal.com/upload/publication/assocFile/BANKING-LAWS-BULLETIN-ISSUE-II_1288782887.pdf
9. Kashyap A. Indian Banking: Contemporary Issues in Law and Challenges. 2014.
10. RBI guidelines focus on fortifying IT security by banks [Internet]. Search Security India; 2011 [cited 2025 Aug 29]. Available from: http://searchsecurity.techtarget.in/news/22400

31005/RBI-guidelines-focus-on-fortifying-IT-security-by-banks
11. RBI for two-stage verification for online banking transactions [Internet]. The Economic Times; 2014 Apr 22 [cited 2025 Aug 29]. Available from: http://articles.economictimes.indiatimes.com/2014-04-22/news/49318793_1_cheque-truncation-system-authentication-transactions
12. Reserve Bank of India. Master Circular on customer service in banks [Internet]. [cited 2025 Aug 29]. Available from: https://rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=8998
13. Reserve Bank of India. Press Release on banking regulations [Internet]. [cited 2025 Aug 29]. Available from: https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=1150816
14. Punjab National Bank v. Rupa Mahajan Pahwa, IV (2015) CPJ 620 (NC).
15. Reserve Bank of India. Press Release on cybersecurity and banking [Internet]. [cited 2025 Aug 29]. Available from: https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=43574
16. Mondaq. Key features of the Personal Data Protection Bill, 2019 [Internet]. 2020 [cited 2025 Aug 29]. Available from: https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019

