GOVERNING CYBERCRIME SURVEILLANCE IN INDIAN BANKING: LEGAL, REGULATORY AND ETHICAL PERSPECTIVES

Pranjul Barche, Maharashtra National Law University, Nagpur

ABSTRACT

The Indian Banking Sector has witnessed immense growth in terms of financial access, financial inclusion, real-time transactions and paperless transactions. All of this is a result of rapid digitalisation and the digital wave ongoing worldwide. However, everything comes at a cost. The transformation has also given rise to enhanced exposure to cybercrimes, be it their scope, frequency or complexity. Ranging from phishing and identity theft, cybercrimes have become more sophisticated with account takeover frauds and large-scale data breaches. Banks and financial institutions are also anxious regarding their customers' trust and reputational or financial loss. Consequently, they have deployed advanced surveillance mechanisms and technologies, including biometric authentication, AI assisted fraud detection systems, device fingerprinting and more. These tools are necessary, effective and unavoidable in prevention and detection of cybercrime in the banking sector. However, concerns regarding personal and financial data privacy and its potential misuse cannot be ignored. Consumers' fundamental right to privacy as recognised in *Justice K.S. Puttaswamy v. Union of India* is at risk of infringement if such surveillance systems are deployed left, right and centre without robust governance measures. Additionally, it may also undermine public trust in the digital financial systems.

This paper studies the intersection of privacy and surveillance within the Indian banking sector, analysing relevant legal frameworks such as the DPDP Act, 2023, RBI's cybersecurity guidelines, and global best practices under GDPR and ISO 27001 and ISO 27701. It evaluates the effectiveness and ethical dimensions of existing surveillance mechanisms in the light of recent case studies in the financial sector. The research recommends a balanced, privacy-by-design approach that ensures transparency in surveillance practices, minimal data processing, informed consumer consent, and the integration of advanced privacy-preserving technologies. The Indian banking ecosystem can strengthen its cybercrime resilience by ensuring adequate ethical safeguards and legal compliance into the deployment of surveillance systems, without compromising the dignity, autonomy, and trust of its customers.

Keywords: Cybercrime, Banking Sector, Privacy, Surveillance Technologies, Data Protection, Financial Fraud, India.

1. Introduction

The Indian banking sector has undergone a profound digital transformation in the past two decades. From mobile banking applications to Aadhaar-enabled payment systems, financial services have moved from the branch to the screen, bringing both unprecedented convenience and heightened risks. Cybercrime has emerged as a parallel industry, targeting not only the financial assets of consumers but also the informational infrastructure of banks. The scale of digital penetration in India-over 1.3 billion Aadhaar enrolments and millions of UPI transactions daily-means that the attack surface is massive, and in many ways uncharted.[1]

The problem is not merely technical; it is also normative. The Apex Court's landmark decision in Justice K.S. Puttaswamy v. The Union of India (hereinafter "RTP") firmly placed privacy within the ambit of fundamental rights, thereby requiring that any form of surveillance or data collection in banking must pass constitutional muster.[2] Yet, banks and regulators increasingly deploy sophisticated surveillance tools-AI-driven fraud detection, biometric authentication, and geolocation tracking-raising concerns about proportionality, transparency, and the limits of lawful monitoring.

This paper examines the delicate balance between two competing imperatives: the need to prevent and detect cybercrime in the banking sector, and the equally pressing duty to safeguard informational privacy of individuals. Specifically, the research explores how surveillance technologies, regulatory frameworks, and judicial pronouncements intersect to create a contested space where efficiency and rights collide. The core questions that animate this inquiry are: How can Indian banking institutions deploy surveillance systems without violating privacy norms? To what extent do current laws and RBI guidelines provide adequate safeguards? And, perhaps most crucially, what ethical and operational principles should guide the adoption of privacy-preserving yet effective surveillance mechanisms?

The discussion is structured thematically, beginning with conceptual foundations, traversing through legal frameworks, assessing technological practices, and concluding with normative recommendations. The aim is not to provide definitive answers, but to sketch a framework for balancing the competing values of security and privacy in a sector that is too vital to be left

[1] RBI, Report on Trend and Progress of Banking in India 2022-23, at 45 (2023).
[2] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

vulnerable.

2. Conceptual Framework

Cybercrime in the banking sector is not a monolithic phenomenon; it is a constellation of activities ranging from phishing and identity theft to advanced persistent threats against banking servers. The Indian CERT-In reported nearly 1.4 million cyber incidents in 2022, a substantial fraction of which targeted financial institutions.[3] While statistics often underrepresent the real scale-owing to underreporting by banks concerned with reputational risk-they provide a baseline to understand the scope of the challenge.

From a definitional standpoint, cybercrime against banks may be viewed through two lenses: (a) crimes "of" technology, where the system itself is attacked (e.g., DDoS attacks, malware injections), and (b) crimes "through" technology, where the banking system is exploited as a conduit (e.g., fraudulent UPI transfers).[4] Both categories implicate not just financial loss but also erosion of consumer trust, which in banking is a form of capital arguably more valuable than liquidity itself.

Privacy, on the other hand, occupies an ambivalent position in this discourse. In the constitutional sense, privacy entails control over personal information and autonomy in decision-making.[5] Yet in the practical context of banking, privacy often translates into data confidentiality and secure authentication mechanisms. Banks are custodians of sensitive personal data, including biometric identifiers, credit histories, and geo-location footprints. This custodianship imposes a fiduciary-like duty-although not formally articulated as such in Indian jurisprudence-to prevent misuse, whether by external actors or internal surveillance systems.

The conceptual tension arises when privacy and surveillance collide. Surveillance is framed by regulators as a necessary instrument to detect anomalies in financial transactions. For example, Section 12 of the PMLA (PMLA) obliges banks to maintain and report records of transactions that may appear suspicious.[6] However, the same act of recording and analyzing transaction trails may also constitute intrusive profiling if unchecked by safeguards.

---

[3] Indian Computer Emergency Response Team, *Annual Report 2022*, at 18 (2023).
[4] Jonathan Clough, *Principles of Cybercrime* 45–46 (2d ed. 2015).
[5] Gautam Bhatia, *Privacy and the Right to Privacy in India: A Constitutional Biography*, 9 Indian J. Const. L. 123, 130–31 (2018).
[6] PMLA, No. 15 of 2003, S. 12 (India).

The jurisprudential difficulty is that while cybercrime prevention is a legitimate aim of the state, the means adopted must conform to constitutional proportionality standards. In India, proportionality requires (i) a legitimate state objective, (ii) suitability of means, (iii) necessity in the absence of less restrictive alternatives, and (iv) a balancing of interests.[7] Applying this test to banking surveillance is not straightforward. For instance, AI-driven systems that monitor spending behavior for anomalies may be effective, but their opacity and potential for false positives raise concerns under the necessity and balancing prongs.

Thus, the conceptual framework that guides this study situates cybercrime and privacy not as binary opposites but as values in constant negotiation. Preventive technologies cannot be rejected outright, nor can privacy be diluted to a token safeguard. The task, therefore, is to seek frameworks-legal, technological, and ethical-that allow coexistence rather than dominance of one value over the other.

3. Legal & Regulatory Framework

The Indian legal framework addressing cybercrime in the banking sector is dispersed across multiple statutes, regulations, and judicial interpretations. Unlike some jurisdictions that have enacted a comprehensive financial cybersecurity law, India relies on a patchwork system: the IT Act, 2000, the RBI's regulatory guidelines, sectoral statutes like the PMLA, 2002, and more recently, the DPDP Act, 2023. This multiplicity has strengths in flexibility but also weaknesses in clarity and coherence.

3.1 The Information Technology Act, 2000

The IT Act remains the core of India's cyber-law regime. Sections 43 and 66 criminalize unauthorized access, hacking, and damage to computer resources, which directly covers attacks on banking servers.[8] Section 66C and 66D, dealing with identity theft and cheating by impersonation, are particularly relevant for banking frauds conducted via phishing or false electronic communications.[9]

However, enforcement under the IT Act has been inconsistent. One practical difficulty lies in attributing liability. In a phishing scam where funds are siphoned through multiple mule

[7] *Modern Dental College & Research Centre v. State of M.P.*, (2016) 7 SCC 353, 60.
[8] IT Act, No. 21 of 2000, S. 43, 66 (India).
[9] Id. S. 66C–66D.

accounts, pinning culpability on the original perpetrator is often technologically challenging. The Act, though forward-looking at the time of its enactment, has not fully caught up with financial technologies like UPI or blockchain-based settlement systems. Scholars have often noted that the IT Act is "remedial, not preventive" in its orientation, leaving a regulatory vacuum in areas like proactive threat monitoring.[10]

3.2 RBI's Regulatory Mandate

As the banking regulator, the RBI has issued a series of guidelines on cybersecurity and customer data protection. The Cyber Security Framework for Banks (2016) requires banks to establish Security Operations Centers (SOCs), conduct vulnerability assessments, and report major incidents to the RBI within two to six hours.[11] Similarly, the circular of RBI on "Storage of Payment System Data" (2018) mandates that all payment data be stored only in India, reflecting a sovereignty-driven approach to data governance.[12]

In practice, compliance has been uneven. Large public-sector banks often struggle with legacy IT systems, making full adherence technically difficult. Private-sector banks, conversely, tend to adopt advanced monitoring tools but sometimes prioritize efficiency over customer privacy. RBI's supervisory inspections (SPARC framework) reveal repeated lapses in incident reporting, indicating that the regulatory "stick" is more symbolic than coercive.

3.3. The PMLA and Transaction Surveillance

The PMLA imposes obligations on banks to retain transaction details and furnish reports on suspicious activities to the Financial Intelligence Unit (FIU-IND).[13] While designed to combat money laundering and terrorism financing, the framework indirectly enhances cybercrime surveillance. Yet it also creates tension with privacy guarantees. The mandatory collection of Know Your Customer (KYC) information-Aadhaar, PAN, biometric identifiers-means banks hold some of the most sensitive datasets in India.

Judicial interpretation has reinforced this expansive surveillance mandate. In *Binoy Viswam v. Union of India*, the Apex Court upheld the mandatory linkage of PAN with Aadhaar for tax

[10] Pavan Duggal, Cyberlaw in India 112–14 (3d ed. 2019).
[11] RBI, *Cyber Security Framework in Banks* (2016).
[12] RBI, Circular on *Storage of Payment System Data*, RBI/2017-18/153 (2018).
[13] PMLA, No. 15 of 2002, S. 12 (India).

purposes, while cautioning that data protection principles must be preserved.[14] The Court's language is at times aspirational rather than enforceable, which creates a gap between constitutional ideals and regulatory practice.

3.4. Data Protection and Privacy Law

The recently enacted DPDP Act, 2023, is India's first comprehensive data protection statute. It recognizes consent, purpose limitation, and storage limitation as guiding principles for processing personal data. For banks, this implies stricter accountability in how customer data is collected and shared. Section 8 of the Act requires "reasonable security safeguards" to prevent data breaches, a provision that could potentially impose liability for large-scale banking leaks.[15]

Nevertheless, the Act contains broad exemptions for government agencies on grounds of national security and public order.[16] Since financial surveillance is often justified under these headings, there is an inherent risk that privacy rights may be subordinated in practice. Critics argue that the Act does not sufficiently empower customers to seek remedies against either state or private actors.

3.5 Constitutional Overlay

The constitutional right to privacy, places an overarching constraint on surveillance practices.[17] The judgment affirmed informational privacy as part of Article 21, subject to the proportionality test. Applied to banking surveillance, this doctrine suggests that measures like mandatory reporting of all transactions above a threshold may pass scrutiny, but indiscriminate profiling of customers without clear safeguards may not.

Yet Indian courts have been hesitant to rigorously enforce these standards in financial regulation cases. For instance, while *Puttaswamy* set high benchmarks, subsequent cases involving Aadhaar authentication for welfare schemes show a more deferential posture to state objectives.[18] This inconsistency mirrors a larger judicial struggle: balancing financial integrity

[14] *Binoy Viswam v. Union of India*, (2017) 7 SCC 59.
[15] DPDP Act, No. 22 of 2023, S. 8 (India).
[16] Id. S. 17.
[17] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 .
[18] *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1.

with privacy in a rapidly digitizing economy.

3.6 Comparative Perspective

Globally, frameworks such as the EU's GDPR and the U.S. Gramm-Leach-Bliley Act (GLBA) illustrate alternative models. The GDPR imposes strict obligations on banks to notify data breaches within 72 hours, backed by heavy penalties.[19] The GLBA, conversely, emphasizes consumer privacy notices and safeguards but is more flexible in enforcement. India's hybrid approach borrows elements from both but lacks the enforcement bite of the GDPR.

3.7 Observations

The regulatory landscape is thus fragmented. While statutes and guidelines exist, their implementation often oscillates between overreach (mass surveillance under KYC) and under-enforcement (weak deterrence for cyber frauds). A coherent framework aligning RBI regulations, IT Act provisions, and constitutional privacy standards remains elusive. The challenge is not absence of law but the absence of integration.

3.8 Global References

International benchmarks provide both inspiration and caution for India's regulatory trajectory. The GDPR represents the most comprehensive privacy law globally, embedding principles such as data minimization, purpose limitation, and lawful processing.[20] While India's DPDP Act borrows certain elements, GDPR's stringent enforcement mechanisms-like heavy fines and the role of data protection authorities-are not mirrored with equal strength.

The U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001 provide operational models for risk management and information security. Indian banks, particularly those with international linkages, often align their practices with these standards to satisfy both domestic and cross-border compliance requirements.

Additionally, the Financial Action Task Force (FATF) sets global guidelines on anti-money laundering (AML) and counter-terrorism financing (CFT), requiring banks to implement

[19] GDPR (EU) 2016/679, art. 33.
[20] GDPR (EU) 2016/679 (General Data Protection Regulation).

suspicious transaction monitoring systems.[21] While these obligations strengthen detection, they also heighten surveillance, raising questions of proportionality and individual rights.

Taken together, the Indian and global frameworks reveal a constant tension, that is, regulators and banks must strike a balance between ensuring financial integrity and preserving personal privacy. The absence of a harmonized enforcement mechanism across statutes and regulators remains a key challenge, leading to overlaps, gaps, and occasional regulatory conflicts.

4. Surveillance Technologies in the Indian Banking Sector

The expansion of digital banking has compelled financial institutions in India to deploy increasingly sophisticated surveillance technologies to combat cybercrime, ensure regulatory compliance, and safeguard consumer trust. These technologies, however, exist in a delicate equilibrium with concerns about individual privacy and data protection.

4.1. Biometric Authentication and Identity Verification

India's financial ecosystem is deeply integrated with the Aadhaar framework, which provides biometric-based authentication (fingerprint, iris scan, facial recognition) for customer verification under the *Know Your Customer (KYC)* norms.[22] The Aadhaar-enabled Payment System (AePS) allows transactions using only biometric data, making banking accessible even in rural areas. However, data breaches and unauthorized use of Aadhaar-linked databases have raised concerns about excessive state-enabled surveillance and private misuse of biometric information.[23]

In parallel, banks are adopting advanced facial recognition technologies for secure access to mobile banking apps and ATMs. While these methods enhance security, they also risk creating permanent identifiers, which, unlike passwords, cannot be changed once compromised.

4.2. Transaction Monitoring Systems

Banks implement Artificial Intelligence (AI) and Machine Learning (ML) based monitoring tools to analyze customer transaction patterns, identify anomalies, and flag potential fraud or

[21] Financial Action Task Force, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" (FATF Recommendations, 2021).
[22] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
[23] *K.S. Puttaswamy v. Union of India (Aadhaar case)*, (2019) 1 SCC 1.

money laundering activities.[24] For example, unusual login locations, sudden large transfers, or deviations from a customer's historical behavior can trigger red flags.

The RBI's guidelines on digital lending (2022) mandate robust monitoring of loan disbursements and collections, thereby extending surveillance into the credit ecosystem.[25] These technologies aid in compliance with AML and CFT obligations under the PMLA, 2002, and FATF recommendations. However, algorithmic surveillance raises questions of bias, false positives, and opaque decision-making, where individuals may face wrongful blocking of accounts without adequate redressal mechanisms.

4.3. Device and Network Surveillance

With the growth of mobile banking, financial institutions increasingly rely on device fingerprinting, geolocation tracking, and IP monitoring to prevent unauthorized access. These tools allow banks to verify whether a login attempt originates from a previously trusted device or a suspicious location.[26] While effective against fraudsters, such surveillance may infringe upon location privacy and contribute to the broader debate on whether financial surveillance veers into profiling.

In addition, banks employ multi-factor authentication (MFA), often combining SMS OTPs, push notifications, and device binding. Although MFA improves resilience, the RBI has acknowledged security concerns around SMS-based OTPs due to SIM swap frauds and man-in-the-middle attacks.[27]

4.4. Insider Threat and Employee Surveillance

Cybercrime in banking is not always external; insider threats-ranging from data leaks to collusion in fraud-pose serious risks. Banks employ employee activity monitoring systems, such as keystroke logging, email scanning, and role-based access controls, to mitigate internal

[24] Reserve Bank of India, "Report of the Working Group on FinTech and Digital Banking" (2017).
[25] Reserve Bank of India, "Guidelines on Digital Lending," Circular No. DOR.CRE.REC.66/21.07.001/2021-22 (Sept. 2, 2022).
[26] National Payments Corporation of India, "Fraud Risk Management Framework for Digital Payments" (2020).
[27] RBI, "Security and Risk Mitigation Measures for Electronic Payment Transactions," Circular No. RBI/2016-17/111 (Dec. 6, 2016).

risks. These mechanisms enhance accountability but also create ethical dilemmas, as employees operate under constant digital scrutiny.

4.5. Intersection with State Surveillance

Banking surveillance often intersects with state-mandated monitoring. The Financial Intelligence Unit-India (FIU-IND) requires reporting of suspicious transactions, effectively making banks extensions of the state's surveillance apparatus.[28] Moreover, the Centralized KYC Registry consolidates customer data across institutions, raising concerns about aggregation risks and potential misuse. Critics argue that this architecture, if not supported by strong safeguards, could enable disproportionate surveillance that undermines the privacy guarantees articulated in *Puttaswamy*.

4.6. Challenges and Concerns

While surveillance technologies have undeniably reduced instances of phishing, identity theft, and unauthorized transfers, their deployment has triggered multiple concerns:

1. **Data Security Risks:** Centralized repositories, like Aadhaar-linked databases, present high-value targets for hackers.

2. **Over-Surveillance**: Customers risk being treated as perpetual suspects, with every transaction scrutinized.

3. **Due Process and Transparency**: Algorithms flagging transactions may lack transparency, leaving customers without effective remedies.

4. **Regulatory Fragmentation**: Overlapping guidelines from RBI, SEBI, and other regulators complicate compliance and accountability.

Thus, while surveillance technologies are essential tools in the modern banking environment, their unchecked expansion risks eroding public trust and infringing upon individual rights. Striking a balance between innovation, security, and privacy remains an unfinished regulatory challenge in India.

[28] PMLA, 2002, S. 12; Financial Intelligence Unit-India, Reporting Guidelines (2021).

5. Case Studies of Cybercrime and Surveillance Use

5.1 Major Banking Cyber Incidents in India

5.1.1 Cosmos Bank Cyber Heist

One of the most notorious incidents in Indian banking was the Cosmos Bank cyber heist of August 2018, in which hackers siphoned off approximately ₹94 crore in a coordinated international ATM withdrawal scheme across 28 countries.[29] The attackers compromised the bank's SWIFT payment system and cloned hundreds of debit cards, enabling simultaneous withdrawals in multiple jurisdictions.[30] Investigations revealed that the attackers had infiltrated the bank's systems using malware that bypassed the core banking software and redirected authorization requests, effectively tricking the system into approving fraudulent transactions.[31] This incident underscored both the vulnerabilities of legacy IT infrastructure in cooperative banks and the sophistication of cross-border cybercrime syndicates.

5.1.2 Phishing and Identity Theft Cases

Phishing attacks remain the most pervasive cyber threat for Indian banks. According to CERT-In, over 300,000 phishing incidents targeting Indian consumers were reported between 2020 and 2022.[32] These scams often involve fraudulent emails, SMS messages ("smishing"), or cloned websites resembling legitimate bank portals.[33] A case frequently cited is the 2020 State Bank of India phishing campaign, where customers received emails requesting KYC updates, leading to widespread credential theft.[34] In many of these instances, detection mechanisms such as anomaly-based monitoring failed to flag malicious activity until after financial losses were reported by customers.

5.1.3 Large-Scale Data Breaches

Beyond direct fraud, data breaches in financial institutions have exposed sensitive consumer and transactional data. In 2019, the EarlySalary app breach compromised nearly 200,000 users'

[29] See "Cosmos Bank Loses Rs 94 Crore in Cyberattack," *The Hindu* (Aug. 14, 2018).
[30] Id.
[31] Radheshyam Jadhav, "Cosmos Bank Cyber Heist: Malware Attack Bypassed Core Banking System," *Business Line* (Aug. 2018).
[32] CERT-In, *Annual Report 2022–23*, Ministry of Electronics & Information Technology, Gov't of India.
[33] Id.
[34] See "Phishing Scam Targets SBI Customers," Economic Times (July 2020).

financial details, highlighting risks in third-party fintech partnerships.[35] Similarly, the Juspay breach of 2020 leaked card details and metadata of over 100 million users, which later surfaced on darknet forums.[36] These breaches illustrate the supply chain vulnerabilities banks face when outsourcing payment processing or digital services to external vendors. Surveillance systems in such cases are often less effective because the breaches originate in API integrations or vendor-controlled systems, outside the direct monitoring perimeter of banks.

5.2 Surveillance Technologies in Detection and Prevention

Indian banks deploy a variety of surveillance technologies to combat these threats. AI-driven fraud detection systems analyze transaction velocity, geolocation inconsistencies, and device fingerprints to flag suspicious behavior.[37] Biometric authentication, particularly Aadhaar-based verification, has been effective in curbing identity fraud, though it remains controversial from a privacy standpoint.[38] In the Cosmos Bank case, forensic investigators suggested that a real-time Security Information and Event Management (SIEM) system could have detected anomalies in SWIFT message traffic.[39] Likewise, phishing detection increasingly leverages machine learning classifiers that identify fraudulent URLs and alert customers before login attempts.[40] However, the adoption of such technologies remains uneven, with private and large public banks more advanced compared to cooperative or rural banks.

5.3 Observed Gaps and Challenges

Despite technological advances, structural challenges persist. First, smaller banks often lack financial and technical capacity to deploy advanced surveillance systems.[41] Second, regulatory enforcement gaps mean that compliance with RBI cybersecurity frameworks is inconsistent across institutions.[42] Third, surveillance mechanisms often suffer from high false positives, leading to customer friction and undermining trust in digital banking. Finally, the absence of standardized data-sharing protocols between banks, regulators, and law enforcement hampers

[35] "EarlySalary App Data Breach: 200,000 Customers Affected," Indian Express (Mar. 2019).
[36] "100 Million Juspay Records Leaked on Dark Web," Hindustan Times (Jan. 2021).
[37] RBI, *Report on Trend and Progress of Banking in India 2022–23*, Reserve Bank of India.
[38] Usha Ramanathan, "Aadhaar and Its Discontents," *Economic & Political Weekly*, Vol. 52, No. 50 (2017).
[39] CERT-In, "Incident Report on Cosmos Bank Heist," Ministry of Electronics & Information Technology (2019).
[40] Shweta Singh & Arindam Banerjee, "AI-Powered Phishing Detection in Indian Banking," *Journal of Cybersecurity Studies*, Vol. 5, No. 2 (2021).
[41] DSCI, *Cybersecurity Adoption in Indian Banking* (2021).
[42] RBI, *Cyber Security Framework for Banks* (2016; updated 2022).

effective response to coordinated attacks.[43] These gaps indicate that while surveillance technologies have advanced significantly, their efficacy is constrained by uneven adoption, weak institutional capacities, and systemic coordination failures.

6. Privacy Risks and Ethical Concerns

The increasing digitisation of the Indian banking sector has led to extensive deployment of surveillance and monitoring systems, but these innovations are not without significant privacy risks and ethical concerns. While the argument for their necessity is often framed in terms of fraud prevention, anti-money laundering, and cybersecurity resilience, the potential for overreach and harm to informational privacy remains profound.

6.1 Over-Collection and Misuse of Personal/Financial Data

Banks and payment systems collect a staggering volume of personal data, including Aadhaar identifiers, biometrics, transaction histories, and even geolocation information. The DPDP Act, 2023 prescribes data minimisation obligations, yet practical implementation in banking is inconsistent.[44] The tendency to collect data "just in case" creates a repository that is highly vulnerable to misuse, particularly by third-party service providers engaged in outsourced verification or analytics.[45]

The risk of "function creep" using collected data for purposes beyond original consent-has already been identified in Aadhaar-related litigations.[46] Such practices compromise not only privacy but also the fiduciary duty of banks to act in the best interests of their customers.

6.2 Risk of Profiling and Discrimination

AI-driven fraud detection and credit scoring mechanisms often rely on opaque algorithms. While effective in identifying unusual transactions, these systems can inadvertently perpetuate bias. For example, individuals from certain geographic regions or with specific transaction patterns may face heightened scrutiny or automatic blocking of services.[47] Such profiling raises

[43] Financial Stability Board, *Cyber Incident Response and Recovery: Effective Practices* (2020).
[44] The DPDP Act, No. 22 of 2023, § 6 (India).
[45] Rakesh Krishnan Simha, Outsourcing Risks in Indian Banking, *Financial Express* (Feb. 10, 2022).
[46] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 SCC 1 (Aadhaar case).
[47] Nandan Kamath, Algorithmic Bias in Indian Banking, *Indian Journal of Law & Technology*, Vol. 17, 2021, at 142.

ethical concerns, particularly when customers are denied services without adequate explanation or appeal mechanisms.

Algorithmic opacity also complicates accountability. Without transparency obligations, customers are often unaware that they are being profiled, which conflicts with constitutional principles of fairness and non-arbitrariness under Article 14.[48]

6.3 Data Breaches and Insider Threats

Despite regulatory requirements, Indian banks have suffered multiple breaches exposing millions of records. In 2020, the State Bank of India reportedly left sensitive data of customers on an unprotected server, affecting over 400 million records.[49] Insider threats, such as employees misusing access credentials, remain a persistent risk. Even with technological safeguards like multi-factor authentication, insider misuse is difficult to detect without constant monitoring.

The reputational damage from breaches is compounded by inadequate disclosure practices. Unlike the GDPR, which mandates breach notifications, Indian regulations remain less rigorous, leaving many customers unaware when their data is compromised.[50]

6.4 Lack of Informed Consent and Opaque Data-Sharing

Consent in Indian banking systems is often more illusory than real. Customers rarely have meaningful choice; declining consent frequently means denial of essential services.[51] Moreover, consent forms are written in dense legal language, undermining transparency. Data-sharing arrangements between banks, fintechs, and government agencies also occur with limited disclosure to customers.

This opacity erodes trust in financial institutions. Ethical banking surveillance, therefore, cannot exist without mechanisms for genuine, informed consent and user agency over personal data.

---

[48] INDIA CONST. art. 14.
[49] Ravi Prakash Kumar, SBI Exposes Account Data of 422 Million Customers, *India Today* (Jan. 30, 2020).
[50] GDPR (EU) 2016/679 (General Data Protection Regulation), art. 33.
[51] Usha Ramanathan, Aadhaar: From Voluntary to Mandatory, *Economic & Political Weekly*, Vol. 52, No. 21 (2017), at 5.

7. Balancing Privacy and Surveillance

The dilemma between enabling robust surveillance for cybercrime prevention and safeguarding individual privacy remains one of the most pressing challenges in India's banking sector. While surveillance mechanisms are indispensable to counter advanced cyber threats, unchecked data collection and monitoring may lead to intrusive practices, undermining civil liberties and public trust. This chapter explores various approaches and technologies aimed at achieving a balance.

7.1 Privacy-by-Design in Banking Surveillance

Privacy-by-Design (PbD), introduced by Ann Cavoukian, advocates embedding privacy principles at the initial design stage of systems rather than treating them as an afterthought.[52] In banking surveillance, this means developing fraud detection and monitoring systems that minimize personal data collection, employ anonymization techniques, and restrict access to sensitive records. For instance, India's Aadhaar-enabled payment ecosystem has been criticized for insufficient privacy safeguards.[53] A PbD framework could enforce stricter data minimization and encryption mechanisms while ensuring system interoperability. Banks must also adopt audit trails and accountability measures, reducing the risk of insider misuse. This approach aligns with the proposed Indian Data Protection Bill, which emphasizes privacy as a core design principle in digital infrastructure.[54] The challenge, however, lies in operationalizing these ideals within existing legacy banking systems, which often lack modular adaptability.

7.2 Proportionality in Data Collection

The principle of proportionality-widely recognized in constitutional jurisprudence-requires that surveillance measures be necessary and the least intrusive means to achieve legitimate goals.[55] In the banking sector, this principle translates to collecting only transaction data essential for fraud detection, rather than extensive profiling of consumer behavior. Courts in India have emphasized that proportionality must guide state surveillance.[56] Extending this reasoning, financial institutions should adopt a graded approach, where high-risk transactions are subject to enhanced monitoring, while routine transactions face minimal scrutiny. The RBI, through

[52] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (2011).
[53] Usha Ramanathan, Aadhar and Privacy Concerns, 9 *Indian J.L. & Tech.* 1 (2013).
[54] The DPDP Bill, 2023, Bill No. 150-C of 2023 (India).
[55] Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations* (2012).
[56] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

its cybersecurity framework, implicitly endorses proportionality by mandating risk-based security controls.[57]

7.3 Consent Management Frameworks

Consent is a cornerstone of data protection, yet in banking, customer agreements are often lengthy, opaque, and couched in legal jargon.[58] A robust consent management framework can enhance transparency and user autonomy. Tools like "dynamic consent," which allow users to modify their preferences over time, could be integrated into mobile banking apps. For example, India's Account Aggregator framework provides a model for granular consent where customers authorize data sharing through standardized APIs.[59] However, the effectiveness of such systems depends on consumer awareness and ease of revocation. Without clear exit mechanisms, consent risks degenerating into a mere formality. Thus, operationalizing consent requires both legal mandates and consumer-friendly technological solutions.

7.4 Privacy-Preserving Technologies

Emerging privacy-preserving technologies offer promising avenues for reconciling surveillance with privacy protection.

7.4.1 Homomorphic Encryption

Homomorphic encryption permits operations to be performed directly on encrypted datasets, thereby enabling banks to undertake fraud detection analytics without the need to reveal underlying sensitive information.[60] Although computationally expensive, pilot projects in Europe demonstrate its feasibility for real-time financial monitoring. Its adoption in India would require significant investment in infrastructure but could drastically reduce the risks associated with insider threats and unauthorized data access.

7.4.2 Federated Learning

Federated learning allows a consortium of banks to jointly train machine-learning models while

[57] RBI, *Cyber Security Framework in Banks* (2016).
[58] Graham Greenleaf, Consent in Data Privacy Law, 3 *Asian J. Comp. L.* 1 (2008).
[59] Reserve Bank of India, *Master Direction - NBFC - Account Aggregator (Reserve Bank) Directions* (2016).
[60] Craig Gentry, Fully Homomorphic Encryption Using Ideal Lattices, 9 *Proc. ACM STOC* 169 (2009).

ensuring that raw customer datasets remain localized and undisclosed.[61] Instead, only model updates are exchanged, preserving confidentiality. This is particularly relevant for detecting cross-bank fraud schemes in India, where fragmented data silos hinder intelligence sharing. Adoption of federated approaches could be encouraged under RBI supervision, thereby balancing inter-institutional cooperation with privacy safeguards.

7.4.3 Differential Privacy

Differential privacy introduces controlled statistical "noise" into datasets, preventing the re-identification of individuals while retaining aggregate utility.[62] U.S. institutions like Apple and the U.S. Census Bureau already employ this technique. For Indian banks, differential privacy could support trend analysis on digital lending patterns without compromising consumer identities. However, its success requires strong technical expertise and alignment with India's data protection law once enacted.

8. Recommendations and Proposed Framework

Building upon the analysis in previous chapters, this section proposes a multi-layered framework combining legal, operational, and technological solutions.

8.1 Policy Recommendations for Regulators (RBI, MeitY)

Regulators should introduce sector-specific guidelines under the forthcoming DPDP Act, with clear law for surveillance in the banking sector. RBI must update its cybersecurity circulars to incorporate privacy-preserving technologies and mandate independent audits.[63] The MeitY should collaborate with financial regulators to standardize consent architecture across fintech platforms. Additionally, a statutory requirement for prompt breach notification should be introduced, similar to the GDPR's 72-hour rule.[64] Importantly, coordination between RBI and CERT-In must be institutionalized to create a unified national cyber incident response system for the financial sector.

[61] Qiang Yang et al., Federated Machine Learning: Concept and Applications, 10 *ACM Trans. Intell. Sys. & Tech.12 (2019).*
[62] Cynthia Dwork, Differential Privacy, 33 *ICALP Proceedings* 1 (2006).
[63] RBI, *Master Direction on Digital Payment Security Controls* (2021).
[64] GDPR (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).

8.2 Operational Guidelines for Banks

Banks must adopt layered security with real-time monitoring, but also integrate PbD principles. Recommendations include: anonymization of routine transaction logs; periodic privacy audits; mandatory privacy impact assessments for new digital products; and stronger grievance redressal mechanisms.[65] Insider threats should be mitigated through role-based access controls and continuous staff training. Moreover, banks should implement federated analytics to pool intelligence without breaching customer confidentiality. Integration with the National Cyber Coordination Centre can help banks gain timely threat intelligence. Ultimately, operational compliance should be incentivized through reduced insurance premiums for institutions with superior privacy safeguards.

8.3 Integration of International Best Practices

India can draw lessons from the GDPR, particularly in proportionality, consent, and breach notifications.[66] The U.S. Gramm-Leach-Bliley Act demonstrates effective sector-specific data security obligations, while Singapore's Monetary Authority has pioneered privacy-friendly fintech guidelines.[67] For India, adopting hybrid standards-leveraging GDPR's rigor with the contextual flexibility of Singapore-would be most effective. Furthermore, cross-border cooperation treaties for cybercrime investigations should be expanded, especially under the Budapest Convention framework. Though India has not signed it, aligning domestic laws with its principles can strengthen international collaboration.

8.4 Consumer Awareness and Digital Literacy Initiatives

Even the most robust frameworks fail without informed consumers. Public awareness campaigns-similar to those used for UPI fraud prevention-must emphasize phishing detection, secure password practices, and consent rights.[68] Digital literacy should be integrated into financial inclusion programs, ensuring that rural and first-time users of banking apps are not disproportionately vulnerable. Banks could leverage gamified learning modules within apps to increase engagement. Ultimately, a privacy-conscious consumer base strengthens systemic

[65] International Association of Privacy Professionals, *Privacy Impact Assessments: A Guide* (2020).
[66] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (2013).
[67] Monetary Authority of Singapore, *FinTech Regulatory Sandbox Guidelines* (2016).
[68] Reserve Bank of India, *Be(A)ware – A Booklet on Modus Operandi of Financial Frauds* (2021).

resilience against cybercrime, reducing dependence solely on regulatory oversight.

9. Conclusion

9.1 Summary of Findings

This paper examined the tension between surveillance-based cybercrime prevention and privacy protection in the Indian banking sector. It analyzed major cyber incidents, the role of surveillance technologies, and privacy risks under India's evolving legal framework. The findings demonstrate that while surveillance is indispensable, unregulated practices compromise individual rights. Case studies such as the Cosmos Bank heist illustrate the severity of systemic vulnerabilities. At the same time, the Puttaswamy judgment provides constitutional grounding for proportionality in data collection. Emerging privacy-preserving technologies-homomorphic encryption, federated learning, and differential privacy - offer feasible pathways to reconciliation if adequately supported by law and policy.

9.2 The Way Forward

Going forward, India must institutionalize a privacy-conscious surveillance ecosystem in banking. This requires syncing DPDP Act with RBI's cybersecurity mandates, ensuring that proportionality, consent, and accountability remain guiding principles. Banks should operationalize privacy-by-design while adopting global best practices tailored to local realities. Ultimately, striking this balance is not only a legal necessity but also a trust-building exercise crucial for the digital economy. The integration of privacy into the DNA of Indian financial surveillance, we can achieve dual objectives: resilient banking infrastructure and the protection of fundamental rights.